Univerzita Hradec Králové

Fakulta informatiky a managementu

Protokol TRILL a jeho využití v sítích LAN

Diplomová práce

Autor: Bc. Jonáš Horáček

Studijní obor: Informační management

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové září 2021

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury či zdrojů.

Podpis:

V Hradci Králové dne 16.08.2021 Jonáš Horáček

Poděkování:

Děkuji svému vedoucímu diplomové práce, panu Mgr. Josefu Horálkovi, Ph.D., za poskytnuté konzultace, které mi pomohly s postupem k vypracování bakalářské práce.

Anotace

Cílem této diplomové práce je podrobně popsat principy protokolu TRILL a analyzovat možnosti jeho nasazení v podnikové síti. V teoretické části se podrobně představí principy fungování protokolu TRILL. Bude připravena simulace fungování protokolu TRILL a jeho využití v podnikové síti. V praktické části se vytvoří case study pro nasazení protokolu TRILL s důrazem na vysokou dostupnost požadovaných služeb.

Annotation

Title: TRILL protocol and its use in LANs

The main reason of this master thesis is to desribe principles of the TRILL protocol and analyze the possibilities of its deployment in a corporate network. The theoretical part will introduce in detail the principles of operation of the TRILL protocol. A simulation of the operation of the TRILL protocol and its use in the corporate network will be prepared. In the practical part, a case study will be created for the implementation of the TRILL protocol with emphasis on the high availability of the required services.

Obsah

Úvod

Počítačová síť je jeden velký svět, bez kterého se v dnešní době neobejde téměř nikdo. Vzhledem k tomu, že se jedná o tak rozsáhlé a nezbytné odvětví, je nutné ho nějak systematicky udržovat a rozvíjet. Kdyby se tak nekonalo, nikdy by koncept počítačových sítí nebyl tam, kde je dnes.

V počítačových sítích typu LAN (Local Area Network) s technologií Ethernet, se vyskytují nevyžádané smyčky, které je nutno odstraňovat, jinak by docházelo k zahlcení počítačových sítí, obzvláště v těch rozsáhlých. K eliminaci síťových smyček dlouhodobě slouží síťový protokol STP (Spanning Tree Protocol), u kterého později vznikaly modifikované verze, jako jsou RSTP, MSTP a PVST, případně PVST+. Ovšem nic není dokonalé a není tomu ani jinak u síťového protokolu STP. Například v datových centrech je STP protokol zcela nedostačujícím. Z tohoto důvodu přišel na svět síťový protokol TRILL (Transparent Interconnection of Lots of Links), který ho měl v tomto ohledu nahradit.

TRILL protokol oproti zmíněnému STP protokolu je zvýhodněn podporou libovolných topologií, založených na sítích linkové vrstvy referenčního modelu ISO/OSI, má Fail-safe charakter, využívá nejvýhodnější cesty k dosažení cíle a přenosové kapacity všech linek sítě, roky bývá neustále ve vývoji, a tudíž TRILL protokol nese oproti STP protokolu více předností, které jsou samozřejmě zmíněné v teoretické části této diplomové práce.

V teoretické části jsou podrobně představené principy fungování protokolu TRILL. Jelikož se jedná o protokol, na kterém je celá tato diplomová práce stavěna, jak už i její název říká, tak je jím zahájena přímo první kapitola. Druhá kapitola začíná zmíněným předchůdcem TRILL protokolu, tedy STP protokolem, kde jsou představeny i jeho pokrokovější varianty, konkrétně RSTP, MSTP a PVST či PVST+. Vzhledem k tomu, že TRILL protokol není jediným existujícím řešením, které mělo za úkol nahradit STP protokol, tak ve třetí kapitole jsou představena dvě alternativní řešení, kterými je FabricPath od společnosti Cisco a tím druhým řešením je SPB neboli Shortest Path Bridging, u kterého došlo k důkladnému porovnání.

Čtvrtá kapitola se týká počítačové sítě jako takové, kde je ze začátku obecně popsaná a jelikož je tato diplomová práce zaměřená na využití v sítích typu LAN, jak už říká její název, tak právě proto je jako první typem sítě dle rozsahu představena ve čtvrté kapitole. Následně po ní jsou představeny i zbylé typy sítí, které jsou členěné dle rozsahu. Konkrétně se jedná o sítě PAN, MAN, CAN, GAN a WAN. Ve čtvrté kapitole je popsán i referenční model ISO/OSI a s ním i jeho jednotlivých 7 vrstev, jelikož se jedná o zásadní pojem pro oblast počítačových sítí.

Pátá kapitola se týká virtuálních LAN sítí, tedy VLAN, které jsou využity v praktické části této diplomové práce při simulaci síťové topologie, která odkazuje na podnikovou síť s třívrstvou architekturou.

V šesté kapitole jsou představeny link state routing protokoly, kterými jsou protokol OSPF a protokol IS-IS. TRILL protokol využívá rozšíření IS-IS protokolu a právě z tohoto důvodu jim je věnována tato šestá kapitola.

Sedmá kapitola specifikuje místa, ve kterých je prakticky nejvhodnější realizace protokolu TRILL. Těmi místy jsou datová centra a podnikové sítě.

V praktické části, tedy v osmé kapitole, je představen vybraný simulátor, ve kterém byla vytvořena síťová topologie pro simulaci podnikové sítě. Tímto vybraným simulátorem je program eNSP od společnosti Huawei. V kapitole je kromě jeho představení i podrobně popsaná jeho instalace, podmínky pro podporu virtualizace, spuštění prostředí a ukázkový příklad topologie, kde je na něm i pospáno, jak se s programem eNSP pracuje a co dělají jednotlivé ovládací prvky v daném prostředí. V neposlední řadě se v této kapitole pro praktickou část nachází vytvořená topologie simulující fungování protokolu TRILL a jeho systematické využití v podnikové síti. V praktické části je vytvořena i následná case study, podle které bylo zjištěno, jak RBridge zařízení nasazené s TRILL protokolem pomáhají podnikové síti, a to v porovnání oproti klasickým switchům typu Ethernet s STP protokolem.

1 TRILL protokol

První představení TRILLu sahá až do roku 2004, kdy se jednalo o pracovní skupinu spadající pro společnost IETF (Internet Engineering Task Force). Neoficiální diskuze ohledně TRILL protokolu se vyskytovali už dříve, někdy kolem roku 2002. V březnu 2010 byl TRILL protokol společností IETF schválen s finálním statusem jako standard. Za vznikem protokolu TRILL stojí paní Radia Perlman, která je mimochodem autorkou původního síťového protokolu STP (Spanning Tree Protocol), kterého TRILL protokol nahrazuje. [3; 4; 11; 14]

TRILL neboli Transparent Interconnection of Lots of Links je síťový protokol, který funguje na sítích druhé vrstvy (L2) referenčního modelu ISO/OSI, tedy na vrstvě linkové. Bývá implementován na základě rozšíření link state routing protokolu IS-IS (**I**ntermediate System to Intermediate System). Síťová zařízení, která slouží k funkci TRILL protokolů se nazývají směrovací mosty, v odborné terminologii Routing bridges (RBs). RBridge kombinuje výhody bridgů a routerů. [5]

TRILL protokol za pomocí link state routing protokolu IS-IS zjišťuje nejkratší cesty mezi switch zařízeními neboli přepínači, na základě přístupu hop-by-hop. Každé RBridge síťové zařízení rozezná veškerá ostatní RBridge zařízení v konkrétní počítačové síti a jejich celkové propojení mezi nimi. Na základě těchto informací lze vypočítat nejkratší cesty ke všem ostatním síťovým uzlům prostřednictvím Shortest Path Tree (SPT) algoritmu. [6]

Protokol TRILL umožňuje realizovat vývoj neblokované síťové architektury, která maximálně poskytuje celkové využití nepostřehnutelných sítí z hlediska uživatele a pomáhá jim zapojit nové servery i v případě, že všechny aktivní kanály jsou redundantní. [8]

Mimo jiné TRILL protokol zahrnuje výhody třetí vrstvy (L3) referenčního modelu ISO/OSI, tedy vrstvy síťové do počítačových sítí fungujících na vrstvě druhé (L2), kde se jedná o vrstvu linkovou. TRILL protokol má své uplatnění především v podnikových sítích a datových centrech. Jeho přednostmi je vysoká škálovatelnost, výkon, rozšiřitelnost a skvělá flexibilita. [9]

Jedná se o technologii, která se zabývá téměř stejnými požadavky jako technologie FabricPath. Tyto dvě technologie jsou si i dost podobné svými výhodami. [1]

1.1 Cíle a přednosti TRILL protokolu

Cílem protokolu TRILL bylo nahradit tehdy dosavadní síťový protokol Spanning Tree Protokol (STP) v sítích Ethernet. Původní tvůrci protokolu TRILL si stanovili tyto cíle ve výchozím dokumentu RFC, tedy konkrétně RFC 5556. [3; 7]

Mezi konkrétní tehdy stanovené cíle patří:

- Využití nejvíce prospěšné cesty ke konkrétnímu cíli
- Podpora libovolné topologie spojů linkové vrstvy (L2)
- Disponovat možností analýzy chování sítě linkové vrstvy (L2) za pomoci patřičných nástrojů
- Využití takzvaného multi-pathingu, kde spoje pro přenos budou souběžné od stejného zdroje ke stejnému cíli

- Využití přenosové kapacity všech spojů pro síť, kde by nemělo dojít k blokování redundantních tras
- Stabilita sítě by měla být zajištěna
- Zacyklení rámců v síti by mělo být poctivě zabráněno
- V případě, že by se jednalo o nejasný stav, musí být konkrétní port zablokován, než aby byl vůbec otevřen. To znamená mít takzvaný „Fail-safe“ charakter
  [3; 7]

Jak už bylo výše zmíněno, TRILL protokol nahrazuje Spanning Tree Protocol (STP), a tak stojí za zmínku i to, že TRILL protokol disponuje určitými aspekty, které dosud v linkové vrstvě (L2) nebyly zvykem. [3]

Mezi takové aspekty patří:

- Využívání distribučních stromů a RPF (Reverse Path Forwarding) kontroly, kde se jedná o kontrolu směrování opačnou cestou při doručování skupinových rámců pro více cílů
- Za pomocí LSRP protokolu IS-IS je využit SPF (Shortest Path First) algoritmus neboli Dijkstrův algoritmus, který pomáhá při hledání nejideálnější cesty v konkrétní počítačové podsíti
- Rámec Ethernetové sítě je zapouzdřen do záhlaví TRILL protokolu a do vnějšího ethernetového rámce. To pomáhá pro zajištění neviditelnosti MAC adres koncových zařízeních u tranzitních switchů
  [3; 13]

TRILL protokol se postupem času vyvíjel s dalšími cíli, mezi které patří například:

- Dosah ECMP
- Konfigurace Plug & Play – konfigurace musí být jednoduchá tak, že TRILL switch (Rbridge) musí mít podobně nenáročnou konfiguraci jako klasický switch
- Zrychlená konvergence pro počítačovou síť a zrychlená obnova v případě, kdy dojde v síti k selhání
- Společná existence se stávající třetí vrstvou (L3) či druhou vrstvou (L2)
- Sjednocený řídící protokol pro vysílání typu unicast a multicast
- Zefektivnit využití síťových spojů
- Podpora virtualizace

- Preventivní opatření proti přetížení tabulky MAC adres
- Zásadně zamezit problémům se smyčkami v síti
- Vylepšit detekční mechanismy
- Podpora sítí typu VLAN (Virtual Local Area Network), priority rámců a 24 bitová datová šířka (což znamená 16 milionů VLAN k dispozici)
- Zachována kompatibilita se současnými routery ze síťové vrstvy (L3)
- Tabulky zaměřené na přesměrování unicast vysílání v průchodných RBridge zařízeních rostou s počtem RBridge zařízeních v sítí, nikoliv s počtem koncových stanic
- Rámec z počítačové sítě typu Ethernet musí být doručen ze zdrojového elektronického zařízení do zařízení cílového takovým způsobem, aby jeho podoba zůstala nezměněná

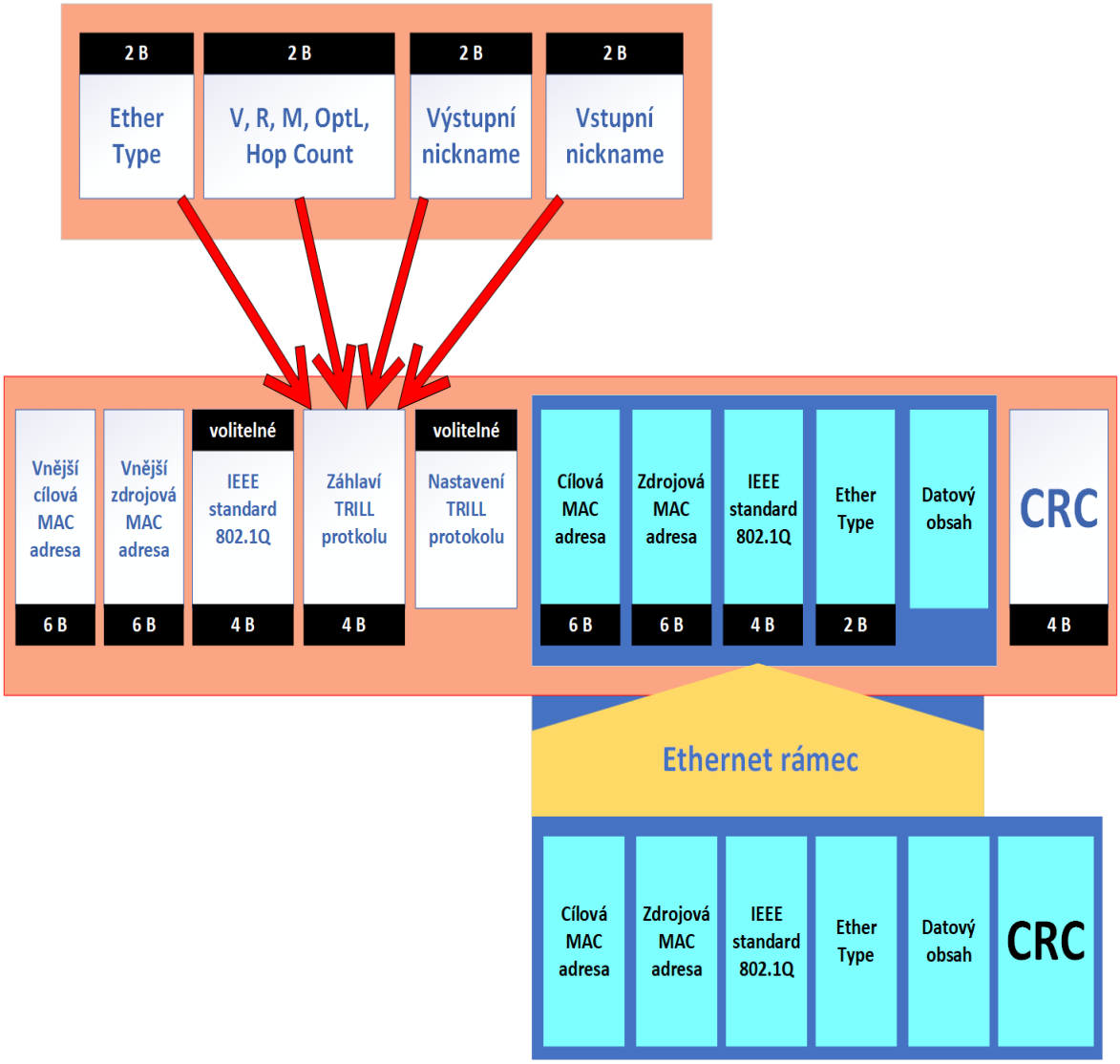
  [1; 11; 12; 13]

1.2 TRILL rámec

Na obrázků č. 1 je znázorněna struktura TRILL rámce, který bývá zasílán mezi aktivními síťovými prvky typu RBridge. Zapouzdření TRILL protokolu je teoreticky stejné jako zapouzdření typu MAC-in-MAC, pouze je doplněné se záhlavím TRILLu mezi nimi. [1]

Vnější zdrojová MAC adresa a vnější cílová MAC adresa odpovídají MAC adrese switche, který se nachází v následujícím úseku a switche ze strany odesílatele.
Tento způsob je podobný i v případě IP adres, kde jsou cílové adresy a zdrojové adresy přepsány na každém následujícím routeru. Vnější zdrojová MAC adresa a vnější cílová MAC adresa mají lokální význam a jsou přepisovány v každém kroku TRILL sítě. [1]

Překryté záhlaví má volitelnou možnost standardu IEEE 802.1q, který je potřeba převážně tehdy, kdy je k síti typu LAN připojeno více aktivních síťových prvků typu RBridge. TRILL záhlaví je přidáno za volitelný standard typu IEEE 802.1q. Standard IEEE 802.1q se skládá z šestnáctibitové hodnoty EtherType a z TCI, tedy Tag Conrol Information. EtherType s hodnotou 0x22F3, v hexadecimální soustavě identifikuje výskyt záhlaví TRILL protokolu. [1]



Obrázek 1 - Struktura TRILL rámce

Přepracováno od zdroje: Hooda – Using TRILL, FabricPath and VXLAN [1]

Vysvětlení jednotlivých elementů z obrázku č. 1:

- **Verze (V):**

  Jedná se o dvoubitové pole, které určuje verzi TRILL protokolu. Příchozí RBridge zařízení vyplňuje toto pole verzí, kterou momentálně spouští. Pokud zařízení RBridge obdrží rámec typu TRILL s číslem verze, které není kompatibilní, tak se rámec zruší. [1]

- **R:**

  Jedná se taktéž o dvoubitové číslo, které ale nebylo využito. [15]

- **M bit:**

  Jedná se o jednobitové číslo, které udává, zda výstupní nickname odpovídá jednomu RBridge zařízení nebo multicastu. V případě, že je rámec nastavený na hodnotu 1, jedná se o rámec určený pro více příjemců a pole pro výstupní přezdívku je dáno distribučním stromem. V opačném případě se jedná o rámec, který je cílený pro jediného příjemce. [1; 15]

- **OptL:**

  Jedná se o pětibitové pole, které určuje délku volitelného záhlaví TRILL rámce. Pokud je hodnota nula, znamená to, že rámec nemá žádné volitelné záhlaví TRILL protokolu. Toto pole určuje délku volitelného záhlaví, v jednotkách od čtyř oktetů, sahající až do maxima pro jedno sto dvacet čtyři oktetů. [1]

- **Hop count:**

  Jedná se o šestibitové pole, které je principem podobné poli TTL (Time To Life) v záhlaví IP paketů v síťové vrstvě (L3). Zdrojové RBridge zařízení nastaví počáteční hodnotu pro toto pole. Každý přechodný RBridge snižuje hodnotu tohoto pole. Pokud je hodnota tohoto pole na nule, tak je paket zahozen a odešle se upozornění na zdrojové RBridge zařízení. Udávaný počet pomáhá řešit problémy způsobené přerušovanými smyčkami, tudíž pakety nemusí procházet sítí navždy. [1]

- **Výstupní nickname:**

  Toto dvoubajtové pole obsahuje přezdívku cílového RBridge zařízení pro rámce vysílání typu unicast a identifikátor distribučního stromu pro rámce, které jsou odesílány pro více cílů. Toto pole není nijak upravené přechodnými RBridge zařízeními. [1]

- **Vstupní nickname:**

  Toto dvoubajtové pole obsahuje přezdívku zdrojového RBridge zařízení a není nijak upravené přechodnými RBridge zařízeními. [1]

- **Nastavení TRILL protokolu:**

  Možnosti pro nastavení jsou k dispozici v závislosti na poli OptL a na základě toho, jestli je v záhlaví TRILL protokolu nenulové, aby byla zajištěna zpětná kompatibilita, tak jsou definovány dva bity, které musí být k dispozici na začátku prvního oktetu oblasti možností. Předmětnými dvěma bity jsou CHBH (Critical Hop by Hop) bit a CltE (Critical Ingress to Egress) bit. [1]

- **CHBH (Critical Hop by Hop) bit:**

  V případě, že je tento bit nastaven na hodnotu jedna, znamená to, že jsou k dispozici některá kritická nastavení typu hop by hop. V případě, že tranzitní RBridge zařízení nepodporují některá kritická nastavení, musí být rámec zrušen. V tom druhém případě, kdy je tento bit nastaven na hodnotu nula, tak tranzitní RBridge zařízení mají možnost přeposílat rámec bez ohledu na to, jestli jsou nebo nejsou určitá nastavení podporována některými RBridge zařízeními. Pokud tranzitní RBridge zařízení nepodporuje žádné nastavení, tak může transparentně přeposílat rámec obcházením záhlaví pro nastavení. [1]

- **CltE (Critical Ingress to Egress) bit:**

  V případě, že je tento bit nastaven na hodnotu jedna, znamená to, že jsou k dispozici některá vstupně-výstupní kritická nastavení. V situaci, kdy je buď CltE bit nebo CHBH bit na nenulové hodnotě, tak cílová RBridge zařízení, která nepodporují některá kritická nastavení zruší konkrétní rámec. V jiném případě, kdy je buď tento bit nebo CHBH bit nastaven na hodnotu nula, znamená to, že cílová RBridge zařízení mají možnost zpracovat rámec bez ohledu na to, jestli jsou nebo nejsou určitá nastavení podporována některými RBridge zařízeními. [1]

- **CRC (Cyclic redundancy check):**

  CRC neboli cyklický redundantní součet je jednou ze speciálních hašovacích funkcí, která se používá pro detekci chyb při přenosu. Detekuje náhodné změny nezpracovaných počítačových dat, která jsou běžně používaná v sítích a na zařízeních určených pro ukládání dat a programu. Zahrnují pevné disky HDD či SSD. CRC funkce se zakládá na binárním neboli dvojkovém dělení, z tohoto důvodu se mu také někdy říká polynomiální kontrolní součet.

  V průběhu CRC kontroly je ke zprávě, kterou je nutno přenést, připojen pevně stanovený počet kontrolních bitů. Přijímače dat přebírají patřičná data tak, jak mají a kontrolují jednotlivé bity, zda neobsahují chyby.

  Přijímače dat matematickou metodou vydedukují kontrolní hodnotu, která je připojena za pomocí nalezení zbytku polynomiálního rozdělení přenášeného obsahu. V případě, že by se mělo jednat o výskyt chyby, tak bude odesláno negativní upozornění s žádostí o opakovaný datový přenos. [16]

1.3 Řídící vrstva

Řídící vrstva spojuje všechny komponenty TRILL protokolu, které nesou podíl zodpovědnosti za tvorbu síťové topologie a rozhodování ohledně směrování závisejícím na linkovém ohodnocení (Cost) nejideálnější cesty v síti. Řídící vrstva TRILL protokolu je založena na link state routing protokolu IS-IS (**I**ntermediate System to Intermediate System), který slouží k výpočtům, ke směrování rámců se používá SPF (Short Path First) algoritmus. [6]

Strom SPF algoritmu je tvořen na základě zpráv typu Link State PDU (Protocol Data Unit). Řídící vrstva tedy spočívá ve výměnách mezi LSP datovými jednotkami (PDU) a mezi RBridge zařízeními, které se používají k výpočtu SPF algoritmu. Na základě toho LSP přenáší informace ve formě TLV (Type, Length, Value), tedy typ, délka a hodnota. TRILL protokol se při směrování odvíjí od link state routing protokolu (LSRP) s doplňující fází výměny nicknamů. [6]

Proces řídící vrstvy začíná nacházením sousedních zařízení a to tak, že port konkrétního RBrdige zařízení odešle zprávu pomocí Hello rámce, který obsahuje prioritu portů, hodnotu podporované MTU (Maximum Transmission Unit) jednotky a seznam nalezených sousedních zařízení. Jakmile nalezené RBridge zařízení obdrží Hello rámec, přidá zdrojovou MAC adresu, tedy adresu odesílatele do svého seznamu sousedních zařízení. Pokud RBridge zařízení obdrží Hello rámec, který obsahuje vlastní MAC adresu (u nalezených sousedů), vyvodí se z toho, že na konkrétním portu funguje obousměrná komunikace a tím je tedy potvrzeno sousedství mezi těmito zařízeními. [6]

Na základě priority portu se pro všechna RBridge zařízení, která jsou ve stejné počítačové síti typu LAN zvolí jedno RBridge zařízení, které bude označováno jako designated RBridge (DRB). Po výměně Hello rámců si RBridge zařízení v dané síti vymění mezi sebou zprávy typu Link State PDU. Tyto zprávy typu Link State PDU obsahují nickname pro konkrétní RBridge zařízení. Každé RBridge zařízení v síti odešle vlastní nickname, společně s názvy nicknamů sousedních RBridge zařízení ve zprávě typu Link State PDU. U RBridge zařízení, která jsou spolu ve stejné síti typu LAN, bude tyto zprávy odesílat jménem ostatních RBridge zařízení pouze jedno konkrétní zařízení, kterým je dříve zmíněny designated RBridge (DRB). Zbylá RBridge zařízení budou odesílat zprávy typu LSP až poté, kdy bude na jiném portu nalezeno nové sousedství nebo až po vypršení časového limitu LSP zprávy. Tímto způsobem je zajištěna datová koherence u designated RBridge zařízení. Na základě informací o sousedních zařízeních a zpráv typu LSP si každé Rbridge zařízení vypočítá svou vlastní směrovací tabulku a sousednost pro každé ostatní RBridge zařízení v topologii pro danou počítačovou síť. [6]

Tyto zjištěné informace budou zaslány na datovou vrstvu, aby byl umožněn výběr na přesun do následujícího úseku (next hop), pro každé hostitelské zařízení na základě směrovací tabulky. Vzájemně vyměněné zprávy se budou skládat ze seznamu všech RBridge zařízení v topologii z dané počítačové sítě s informacemi pro každou z nich. Mezi zmíněné informace patří MAC adresa následujícího úseku, tedy next hopu, nickname hostitelského zařízení, zvolený kořen distribučního stromu a sousedství pro RBridge zařízení. [6]

1.4 Datová vrstva

Datová vrstva TRILL protokolu zpracovává všechny rámce, které putují do cílového zařízení. Tato vrstva umožňuje rozhodování pro směrování na základě záhlaví TRILL rámce a informací cílového zařízení za pomocí dat získaných od řídící vrstvy. Jakmile rámec doputuje k cílovému zařízení, je podle typu daného rámce možné provést tři hlavní rozhodnutí ohledně směrování a těmi jsou:

- Rámec má TRILL záhlaví a podle něj má i danou šestnáctibitovou hodnotu EtherType. V takovém případě je rámec zpracován patřičnou funkcí a rozhodnutí ohledně směrování závisí na informacích obsažených v záhlaví TRILL protokolu.
- Rámec má nativní EtherType, který má zpřístupněný portem cílového zařízení. V takovém případě by měl být rámec zapouzdřen či přesměrován. Pokud je cílem směrování lokální koncové zařízení, tak rámec může být směrován bez zapouzdření.
- Rámec má nativní EtherType, který má zpřístupněný místní síťovou kartou (NIC). V takovém případě by rámec měl být považován za klasický rámec, tedy za rámec bez elementů TRILL protokolu a měl by být přesměrován na port, který nepatří koncovému zařízení jako nativní Ethernet rámec. [6]

Rámec se zpracovává zapouzdřováním, pokud konkrétní rámec odpovídá klasickému EtherType, zdrojem je lokální koncové zařízení a cíl je buď neznámý nebo jím je něco jiného než tedy lokální koncové zařízení. Prvním krokem je určit, zda je cílová adresa známá či naopak. K tomu slouží vyhledávání ve směrovací tabulce. [6]

Pokud je ve směrovací tabulce nalezen záznam, který obsahuje nickname cílového koncového zařízení, tak je rámeček zapouzdřen záhlavím TRILL protokolu. Toto doplňující záhlaví stanoví localhost, jako příchozí nickname a cílové koncové zařízení jako výstupní nickname. Rámec je poté přesměrován k následujícímu úseku (next hop), aby se dostal k výstupnímu koncovému zařízení, na základě informací získaných z řídicí vrstvy. [6]

Pokud není nalezen žádný záznam, znamená to, že je rámec duplikován. První kopie je zahlcena na všech portech koncových zařízení. Druhá kopie bude zapouzdřena s konkrétním záhlavím TRILL protokolu. Toto záhlaví udává nickname localhosta jako příchozí nickname a zvolený kořen distribučního stromu jako výstupní nickname. Konkrétní bit vysílání typu multicast uvedený v záhlaví TRILL rámce bude jiný než nula. Tato druhá kopie je poté duplikována a odeslána všem sousedním prvkům ve stromové struktuře, za pomocí unicast vysílání na cílovou MAC adresu. [6]

Jakmile je rámec typu TRILL přijat, jsou dvě možnosti a to takové, že rámec může být vysíláním typu **multicast** nebo vysíláním typu **unicast**. [6]

- Pokud je rámec vysíláním typu **unicast**, provede se kontrola, zda je jeho cíl aktuální koncové zařízení nebo tomu je jinak. Pokud tomu tak je, rámec je zbaven zapouzdření. Jakmile je rámec zbaven zapouzdření jsou k dispozici tři možnosti a těmi jsou:

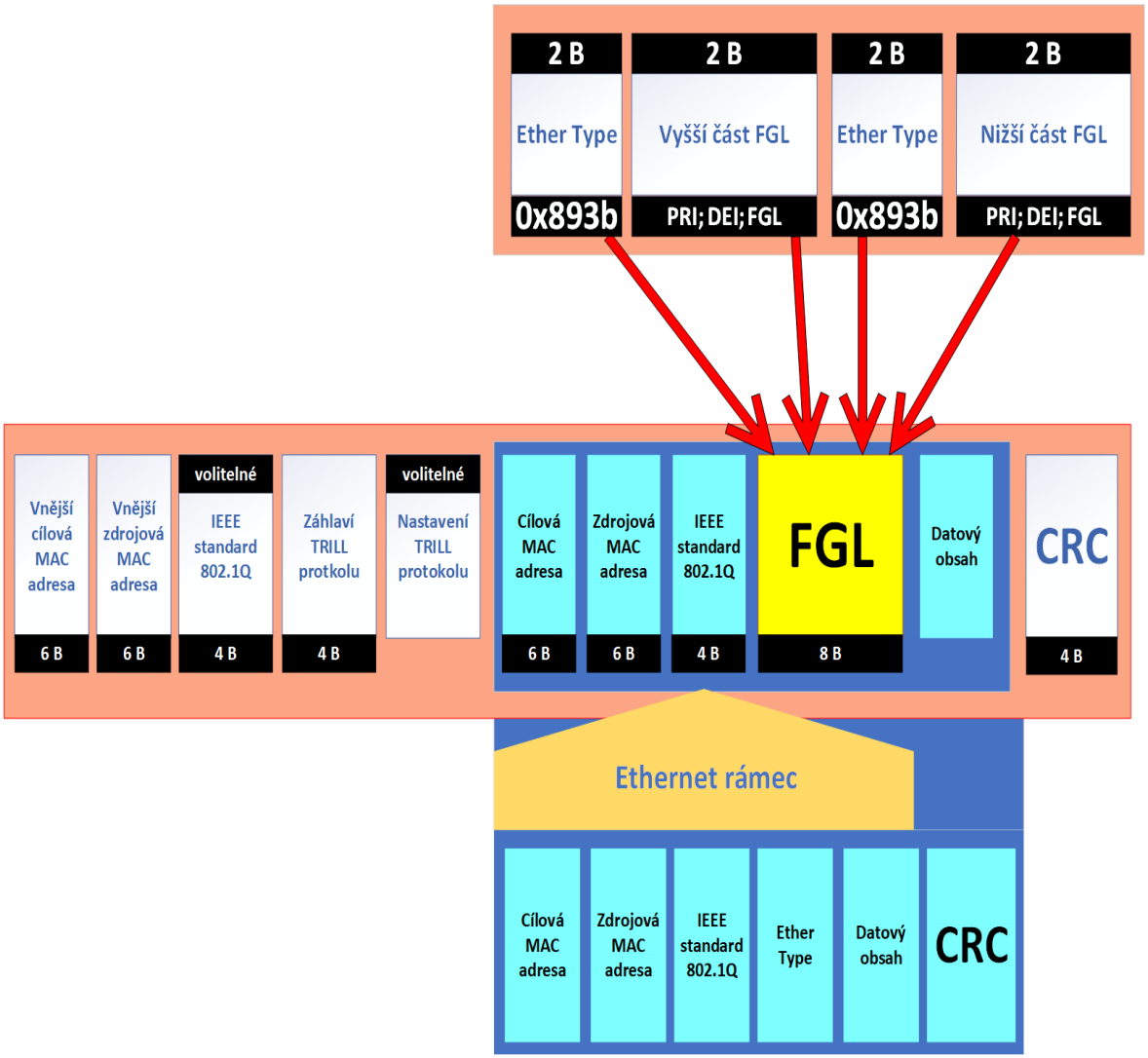
- Pokud je cílem lokální port koncového zařízení, tak je rámec směrován dále. V opačném případě, pokud je cílem lokální port, který nespadá pod koncovému zařízení, je rámec zrušen, aby se zabránilo opětovnému vložení rámce zbaveného zapouzdření do sítě fungující s TRILL protokolem.
- Pokud je cíl neznámý, tak je rámec zahlcen na všech portech koncového zařízení na straně localhosta. Pokud je rámec vysíláním typu unicast a localhost a zároveň není cílovým hostitelským zařízením, a zda informace ohledně cílového hostitelského zařízení existují v databázi na straně localhosta, tak je potom rámec směrován na další úsek v síti, tedy next hop a hodnota počtu úseků (hop count) se sníží o jedničku. To se děje z toho důvodu, aby rámec doputoval k patřičnému cíli. Pokud localhost nemá žádné informace o cílovém zařízení, tak se rámec zahodí. [6]

- Pokud je rámec vysíláním typu **multicast**, uskuteční se kontrola ohledně toho, jestli kořen distribučního stromu (v tomto případě výstupní nickname) zaznamenán v seznamu. V případě, že kořen distribučního stromu neodpovídá výsledkům kontroly nebo se jedná o neznámou hodnotu, tak se rámec taktéž zahodí. V opačném případě, kdy je uskutečněná kontrola ohledně kořene distribučního stromu vyhodnocena úspěšně, tak se rámec duplikuje a hodnota počtu úseku (hop count) se sníží o jedničku.
  První kopie rámce je směrována na všechna sousední zařízení localhosta ve stromové struktuře a hlavně na jejím kořenu. Výjimkou je pouze zařízení, které odeslalo původní rámec. Druhá kopie rámce se zbaví zapouzdření a směruje se na všechny porty koncového zařízení v dané počítačové síti. [6]

1.5 Fine-Grained Labeling

Fine-Grained Labeling (FGL) je rozšiřujícím polem v záhlaví vnitřního Ethernetu u rámce typu TRILL. Jelikož standard IEEE 802.1q využívá pro logické sítě typu VLAN (Virtual Local Area Network) pouze dvanácti bitový prostor, znamená to, že VLAN sítových prvků může být maximálně 4096. Jelikož datová centra a virtuální zařízení se rozrůstají raketovým tempem, nemusí tak být dvanácti bitový prostor vždy dostačující, a právě proto je FGL rozšíření užitečné. FGL rozšíření u TRILL rámce je dosaženo složením dvou VLAN označení a adresní prostor pro sítě typu VLAN se zdvojnásobí a bude tedy 24 bitový. Což znamená dle výpočtu, že bude k dispozici přibližně šestnáct milionů VLAN síťových prvků. [1]

Tyto informace se do záhlaví TRILL rámce mohou dostat více způsoby. A to tak, že se rozšíří o dva prvky IEEE 802.1q a 24 bitový adresní prostor bude dosažen vstupním a výstupním označením VLAN části. Dalším podobným způsobem může být označení konkrétních rámců existujícím Q-in-Q formátem, toho se dosáhne změnou hodnoty EtherTypu oproti původní hodnotě TRILL rámce. [1]



Obrázek 2 - TRILL rámec doplněný FGL

Přepracováno od zdroje: Hooda – Using TRILL, FabricPath and VXLAN [1]

Na obrázku č. 2 je znázorněna struktura TRILL rámce, jak vypadá doplněný s rozšířením Fine-Grained Labeling (FGL).

Pro účel FGL rozšíření je pro EtherType stanovena v hexadecimální soustavě jiná hodnota a to 0x893b. Doplněk FGL má dvě části, a to část nižší a část vyšší. Obě části jsou dvoubajtové. Dvanáct bitů z každé části je vyhrazeno pro hodnotu FGL a zbylé čtyři bity jsou vyhrazené pro hodnoty polí PRI (Priority field) a DEI (Drop Eligibility Indicator). Hodnota pole PRI má vyhrazené tři bity a hodnota pole DEI má k dispozici poslední jeden bit. [1]

Vstupní RBridge zařízení nese zodpovědnost za označení VLAN sítě v příchozím PDU, za mapování příchozího portu a v případě nutnosti i za veškeré politiky, které jsou použité ve 24 bitovém vyhrazeném prostoru pro doplněk FGL v daném rámci. V případě výstupního RBridge zařízení se nese zodpovědnost za mapování 24 bitového prostoru pro doplněk FGL do patřičného místa pro VLAN, která odpovídá výstupnímu portu. Měla by se brát zřetel na hodnoty doplňku FGL při konfiguraci RBridge zařízení, aby mapování do příslušných portů VLAN sítě bylo bezproblémové. [1]

RBridge zařízení, která neumí pracovat s FGL doplňkem, se odborně nazývají VLAN Labeled (VL) RBridge. RBridge zařízení, která mají implementovaný doplněk FGL jsou spolehlivá pro směrování rámců typu TRILL a případný výskyt narušení při směrování by tak neměl být jejich vinou. Kdežto v případě u VL RBridge zařízeních tomu tak není. [1]

Síťový provoz přicházející od VL RBridge zařízení může bezproblémově procházet skrz RBridge zařízení, která mají implementovaný FGL doplněk. Bohužel obráceně tomu tak není. Z tohoto důvodu by síťový provoz s daty, disponující FGL doplňkem, nikdy neměl procházet skrz VL RBridge zařízení, protože jsou v rámci směrování s FGL doplňkem nespolehlivá. Chování v konkrétní počítačové síti se v takových případech odráží od implementace. Některé implementace mohou procházející rámce zahodit, v případě, že hodnota EtherType neodpovídá standardu IEEE 802.1q (0x8100). [1]

V situaci, kdy se jedná o síťový provoz, který směřuje k více cílům, tak je u VLAN sítě brán zřetel na metodu pruning u distribučních stromů. Pokud dojde k situaci, kdy v průběhu síťového provozu, zařízení typu VL RBridge obdrží jednotku s FGL doplňkem, může to mít za následek, že jednotka bude zahozena či metoda pruning bude fungovat špatným způsobem. Právě proto je nutné zajistit, aby síťový provoz, týkající se FGL doplňku, se vyhýbal zařízením typu VL RBridge. [1]

Nejvíce vyhovující volbou, pro takové zajištění je vylepšit všechny dosavadní zařízení typu VL RBridge tak, aby z nich byly RBridge zařízení, která umí bezpečně fungovat pro FGL doplněk. To ale v praxi nemusí být v každém případě. Z takového důvodu je zapotřebí, aby daná počítačová síť disponující TRILL protokolem, současně podporovala kombinaci VL RBridge zařízení a RBridges zařízení fungující s FGL doplňkem. Koncová zařízení by měla mezi sebou navzájem komunikovat bez ohledu na to, zda se jedná o zařízení typu VL RBridges, či o zařízení typu RBridge s FGL doplňkem. Omezení ohledně

toho, kdy síťový provoz disponující FGL doplňkem nemůže procházet přes VL RBridge zařízení v cestě, lze uvést následovně:

- Mezi každým RBridge zařízením s doplňkem FGL, by měla existovat cesta, ve které by mezi zařízeními nepřekáželo žádné zařízení typu VL RBridge.
- Minimálně jeden distribuční strom by měl mít kořen, který byl pro FGL doplněk bezproblémový.
  [1]

Něčeho takového lze dosáhnout několika způsoby. Začít se může například tím, že RBridge zařízení v rámci protokolu IS-IS oznámí v Link state PDU (LSP) jednotce, zda se jedná o bezproblémovou cestu pro doplněk FGL. Edge RBridge zařízení specifikují seznam zařízení, která jsou bezproblémově kompatibilní s doplňkem FGL.

Jedna z metod se zakládá na tom, že RBridge zařízení korespondující s doplňkem FGL oznámí hodnotu (Cost) spoje připojujícího se k VL RBridge zařízení, které bude mít hodnotu vysokou, v rozsahu ($2^{24} – 2$), což je rozhodně více, něž výchozí hodnota (Cost). [1]

Znamená to, že síťový spoj, který propojuje zařízení RBridge fungující s FGL doplňkem k zařízení typu VL RBridge, je využit pouze v momentě, kdy není žádná jiná cesta k realizaci pro dosažení cíle. Aby tato metoda správně fungovala, tak je důležitým požadavkem to, že RBridge zařízení s FGL doplňkem by správně mělo filtrovat veškerou část síťového provozu, kde je aplikováno FGL rozšíření, aby se zamezilo spojení připojující se k VL RBridge zařízení, které by směrování s FGL doplňkem mohlo pokazit. Pokud je daná počítačová síť dobře navrhnutá s redundantními cestami, tak je možné realizovat společnou existenci obou typů zmíněných RBridge zařízení, tedy VL a těch, které disponují FGL rozšířením. [1]

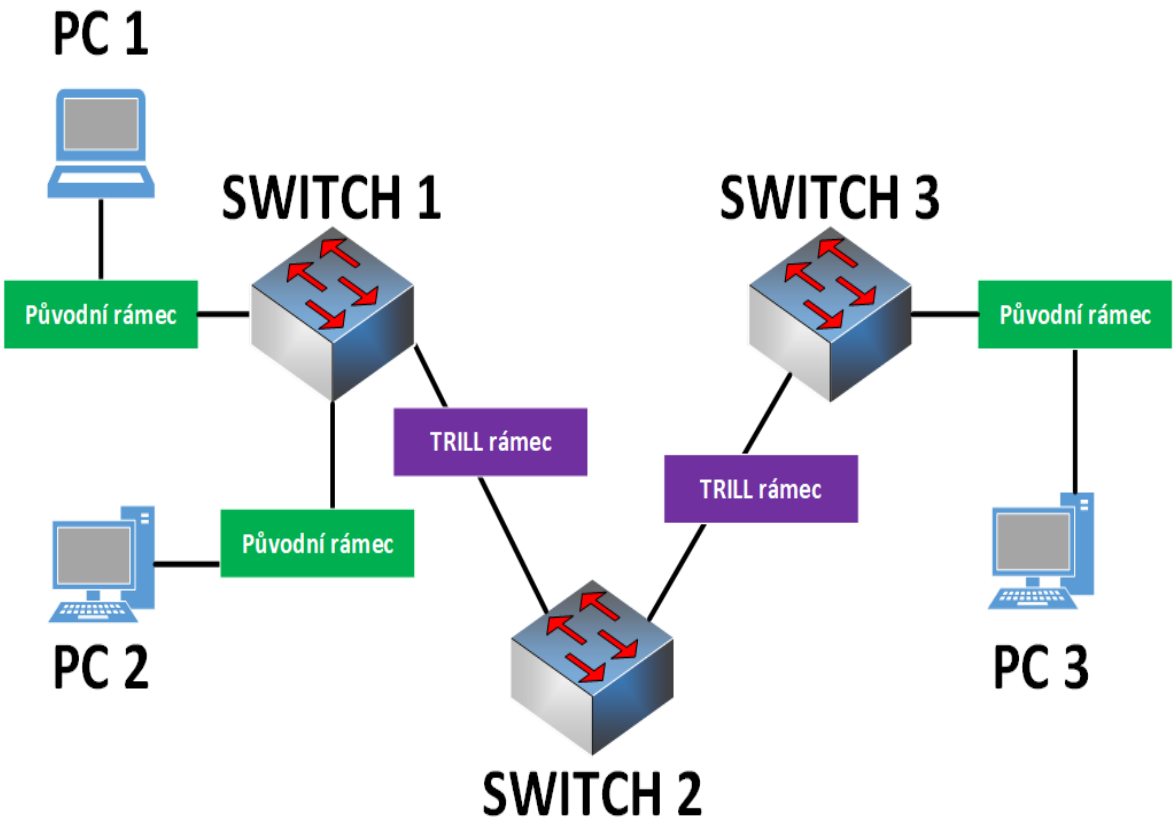
Z této možnosti vyplívá, že jakýkoli síťový provoz obsahující VL RBridge zařízení nejprve projde cestu skrz RBridge zařízení disponující s FGL rozšířením, i přesto, kdy je počet úseků (hop count) vyšší, než je tomu u standardního síťového provozu. Síťový provoz, obsahují VL RBridge zařízení může stále běžet skrz síťový spoj, který má spojovat VL RBridge zařízení a RBRidge s FGL rozšířením v případě, kdy neexistují žádné jiné cesty k dosažení cíle. Musí být brán zřetel na to, aby bylo zajištěno propojení mezi všemi RBridge zařízeními s FGL doplňkem a aby se zamezil průchod při síťovém provozu skrz VL RBridge zařízení. V opačném případě by byl síťový provoz disponující s FGL rozšířením zahozen, kdyby došlo k pokusu vystoupit ze spoje mezi VL RBridge zařízením a mezi RBridge zařízením s FGL doplňkem. [1]

Druha možná metoda se zakládá na případu, kdy RBRidge s FGL rozšířením nemá možnost filtrovat část síťového provozu, kde funguje FGL rozšíření při pokusu vystoupit ze spoje k VL RBridge zařízení. U této metody je tomu podobně jako u metody první, kdy RBridge zařízení korespondující s doplňkem FGL oznámí hodnotu (Cost) spoje připojujícího se k VL RBridge zařízení. [1]

Hodnota zde tentokrát nemá rozsah v hodnotě ($2^{24} - 2$), jako tomu bylo u metody první, ale pouze ($2^{24} - 1$). To znamená, že síťový spoj, propojující zařízení RBridge s rozšířením FGL a se zařízením typu VL RBridge, je blokováno. Ke správné funkci této metody je vhodné, aby počítačová síť zakládající se na TRILL protokolu neměla náhodné kombinace společného propojení VL RBridge zařízení a RBridge zařízeních s FGL rozšířením. RBridge zařízení s FGL rozšířením a VL RBridge by měly být vzájemně od sebe izolovány. [1]

1.6 Ukázka komunikace v síti s TRILL protokolem

Následující obrázek č. 3 znázorňuje zjednodušenou topologii počítačové sítě, ve které fungují tři koncová zařízení a tři switche zakládající se na TRILL protokolu, jedná se tedy o RBridge zařízení (TRILL switche).



Obrázek 3 - Ukázka komunikace s TRILL protokolem

Přepracováno od zdroje: Miroslav Matuška – TRILL 2. část – Základní principy [3]

RBridge číslo 1 a RBridge číslo 3, disponují jak s porty pro koncová zařízení, tak s porty pro připojená RBridge zařízení. Tím se vytváří hranice mezi klasickou počítačovou sítí typu Ethernet a mezi síti zakládající se na TRILL protokolu (TRILL network). RBridge číslo 2 žádné porty s koncovými zařízeními neobsahuje a slouží tedy jako tranzitní RBridge uvnitř sítě s TRILL protkolem. Tabulky pro switche, v tomto případě pro RBridge, ze začátku neobsahují žádné adresy koncových zařízení. [3]

RBridge za pomocí link state routing protokolu IS-IS vypočítají cesty s nejlepší hodnotou (Cost) a také distribuční strom.
Pokud se má poslat rámec ze strany koncové zařízení PC 1 na koncové zařízení PC 2, vyvolá se tím zápis adresy zařízení PC 1 do tabulky RBridge číslo 1 s tím, že se uvede i port, odkud daný rámec na RBridge zařízení přišel. Jelikož cílová adresa pro koncové zařízení PC 2 v tabulce pro RBridge zařízení zatím není, uskuteční se flooding původního rámce na stranu lokálních portů a zároveň i k odeslání rámce se zapouzdřením ve směru distribučního stromu na sousední RBridge číslo 2. [3]

Vzhledem k vyskytnuté situaci, kdy RBridge číslo 2 nezahrnuje žádné porty s koncovými zařízeními, není v takovém případě rámec zbaven zapouzdření ze záhlaví TRILL protokolu a je následně směrován po cestě distribučního stromu na RBridge číslo 3. Před zahájením pro odeslání ještě projde úpravou záhlaví rámce typu TRILL, v případě dalších úprav dojde i k dekrementaci hodnoty počtu úseků (Hop-Count) o jedničku. [3]

RBridge zařízení číslo 3, v daný moment už obsahuje porty s koncovými zařízeními a daný rámec je následně zbaven zapouzdření a dostává se tak do původního stavu. Nejdříve ovšem RBridge zařízení pochytí ze záhlaví TRILL protokolu důležitý postřeh. Tím je myšleno to, že zařízení PC 1 je správně připojené k zařízení RBridge číslo 1. Jelikož cílová adresa zařízení PC 2 není obsažena v tabulce pro zařízení RBridge číslo 3, tak se z toho důvodu uskuteční metoda lokálního floodingu na přímo připojené porty tohoto zařízení. [3]

Pokud se má rámec odeslat ze strany zařízení PC 1 na stranu zařízení PC 3, tak se v takovém případě vyvolá téměř stejná posloupnost kroků. Rozdíl bude pouze ve výsledku. V případě prvním, kdy rámec putuje ze strany zařízení PC 1 na stranu zařízení PC 2, tak je doručen v oblasti lokálního portu stejného RBridge zařízení. V případě druhém, kdy rámec putuje ze strany zařízení PC 1 na stranu zařízení PC 3, tak je doručen na vzdálený RBridge. V obou případech platí situace, že rámec s neznámou cílovou MAC adresou se rozešle na všechna existující místa v dané počítačové síti, kde by se mohlo patřičné cílové zařízení vyskytovat. [3]

Zpětná komunikace ze strany zařízení PC 2 na stranu zařízení PC 1 probíhá stejným způsobem, jako tomu je realizováno na klasickém switchi u sítě typu Ethernet. Poloha MAC adresy pro zařízení PC 1 je už zachycena a zařízení RBridge číslo 1 uskuteční pouze lokální přepnutí daného rámce na port, kam má patřit. Zapouzdření do záhlaví TRILL protokolu se zde neuskuteční. [3]
V rámci zpětné komunikace ze strany zařízení PC 3 na stranu zařízení PC 1, RBridge zařízení číslo 3 už ví, že zařízení PC 1 je připojené k zařízení RBridge číslo 1. RBridge zařízení číslo 3 z takového důvodu realizuje zapouzdření zpětného rámce do záhlaví TRILL protokolu takovým způsobem, aby byl směrován nejvíce ideální cestou na RBridge zařízení číslo 1 bez nutnosti aplikování pomoci formou distribučního stromu. Následně se uskuteční už jen zbavení zapouzdření a rámec se odešle na konkrétní správný port. [3]

2 STP protokol

Algoritmus pro implementaci STP protokolu vynalezla paní Radia Perlman v roce 1985 a poprvé byl praktikován na síťovém bridge zařízení typu Ethernet se dvěma porty. STP protokol funguje jako distribuovaný algoritmus, který pomáhá síťovým bridge zařízením se automaticky přizpůsobit poruchám síťových spojů či instalaci nových síťových bridgů do dané topologie linkové vrstvy (L2). Algoritmus STP protokolu byl zařazen do standardu IEEE 802.1D v roce 1990. V té době sloužil jako jedna z elementárních součástí pro architektury sítí typu LAN. [29]

STP protokol neboli Spanning Tree Protocol slouží primárně k tomu, aby zamezil výskytu smyček v počítačové síti a odpojení redundantních spojů. Jedná se o protokol linkové vrstvy, tedy druhé vrstvy (L2) referenčního modelu ISO/OSI, který funguje na konkrétních aktivních síťových prvcích, kterými jsou zařízení switch a bridge. STP protokol pracuje tak, že předává data tam a zpět, aby zjistil, jakým způsobem jsou switche uspořádány v dané počítačové síti. Následně vezme všechny informace, které shromažďuje, a využije je k vytvoření logického stromu. Některé informace, které STP protokol přijímá, umí definovat, jakým způsobem jsou propojeny všechny switche v dané počítačové síti. [19]

STP protokol takové informace vytváří tím, že odešle síťové pakety, kterým se v tomto případě odborně říká BPDU (Bridge Protocol Data Units). Tyto síťové pakety typu BPDU, respektive data, která jsou v nich obsažena, umí řídit způsob, jakým STP protokol dokáže určit topologii počítačové sítě. [19]

BPDU jednotka u STP protokolu má tři hlavní složky. Mezi ně patří globální informace o STP protokolu, což je například jeho verze. Další složkou jsou informace dané instance STP protokolu pro potřebu konfigurace a poslední složkou jsou parametry časovače neboli STP timers. [24]

Obrázek č. 4 znázorňuje jednotlivé tři složky BPDU jednotky, včetně jejich konkrétních údajů a hodnot v nich obsažených. První složkou z horní části označenou na obrázku č. 4 světle oranžovou barvou jsou globální informace, kam patří verze protokolu, ID protokolu, typ BPDU jednotky a křídlové značky (flags). Druhá složka, která je na obrázku č. 4 označena světle modrou barvou zahrnuje informace dané instance STP protokolu, kam patří hodnota Bridge ID (BID) rootu, hodnota cesty rootu, hodnota Bridge ID (BID) odesílatele a posledním údajem této složky je port ID odesílatele. Poslední složka, která je na obrázku č. 4 označena zelenou barvou, zahrnuje časovače STP protokolu, kterým se odborně říká Spanning Tree timers, spadá tam Max Age, Message Age, Hello Time a Forward Delay.

velikost (uvedeno v Bytech)	údaj
2	ID protokolu
1	verze protokolu
1	typ BPDU
1	flags
8	root Bridge ID (BID)
4	root path cost
8	Bridge ID odesílatele
2	port ID odesílatele
2	Message Age
2	Max Age
2	Hello Time
2	Forward Delay

Obrázek 4 - jednotka BPDU a její složky

Přepracováno od zdroje: Petr Bouška Cisco IOS 9 - Spanning Tree Protocol [24]

Každý switch v dané topologii porovnává patřičné parametry v datové jednotce BPDU, které zasílá svému sousednímu zařízení s parametry z datové jednotky BPDU, které daný switch dostal od svého sousedního zařízení. [21]

U STP protokolu je rozhodující pro všechny switche v dané počítačové síti zvolit konkrétní root bridge, který se v té konkrétní počítačové síti stane hlavním působištěm. Veškerá další rozhodnutí v dané počítačové síti se odvíjí z pohledu toho konkrétního root bridge, který je zvolen na základě hodnoty Bridge ID (BID). [21]

V průběhu procesu pro výběr vhodného root bridge platí hodnocení, že menší znamená lepší výsledek. Pokud například prvnímu switch zařízení náleží nižší číslo hodnoty Bridge ID (BID), než má hodnota Bridge ID (BID) druhého zařízení switch, znamená to, že první switch zařízení je ideálnější volbou stát se root bridgem. [21]

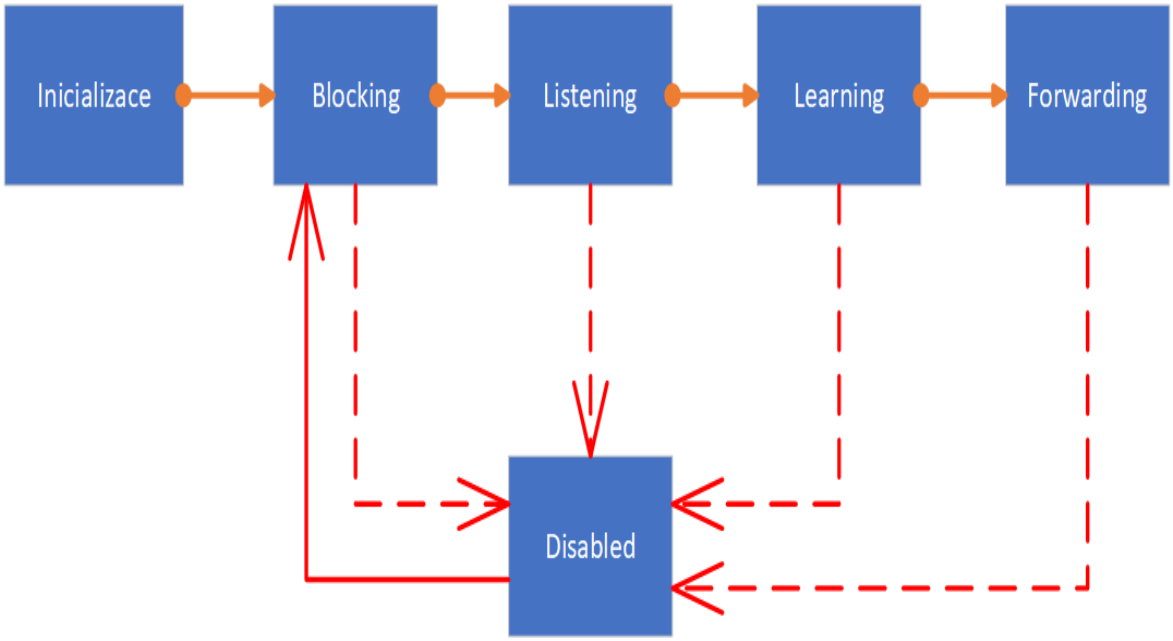
Bridge ID je jednou ze základních hodnot každého switch zařízení. Hodnota se skládá z priority o rozsahu dvou bajtů, hodnota priority je ve výchozím stavu 0x8000 a z MAC adresy konkrétního switche, jejíž rozsah je šest bajtů. Hodnota Bridge ID (BID) lze změnit na základě změny priority konkrétního switch zařízení. [24]

2.1 Stavy portů při STP protokolu

Každý port na switch zařízení, které využívá STP protokol, má vždy svůj určitý stav. Těmito možnými stavy jsou:

- **Disabled** – Jedná se o stav, který se manuálně konfiguruje. V momentě, kdy je port v tomto stavu, tak je zcela nefunkční a nepřijímá ani nepřenáší žádné rámce.
- **Blocking** – V tomto stavu je port v momentě, kdy se nijak nepodílí na směrování rámců, na druhou stranu přebírá zprávy ze strany správy sítě a vytváří na ně odpovědi.
- **Listening** – V tomto stavu port pouze přijímá a odesílá jednotky BPDU a stejně jako předchozí stav Blocking také přebírá zprávy ze strany správy sítě a vytváří na ně odpovědi.
- **Learning** – V tomto stavu je port, který nesměruje žádné rámce, ale zvládá přijímat a odesílat jednotky BPDU, naplňuje směrovací tabulku pro přípravu na směrovací stav (Forwarding). Taktéž jako předchozí zmíněný stav přebírá zprávy ze strany správy sítě a vytváří na ně odpověd.
- **Forwarding** – V tomto stavu port směruje všechny rámce, stejně jako předchozí zmíněný stav Learning, tak i tento stav přijímá a odesílá jednotky BPDU a taktéž přebírá zprávy ze strany správy sítě a vytváří na ně odpovědi.
  [10]

  Následující obrázek č. 5 znázorňuje, jak po změně topologie počítačové sítě či restartu, postupně prochází port při využití STP protokolu skrz výše zmíněné stavy. Stavy, kterými port využívající STP protokol projde, před zahájením směrování postupují následovně: ze stavu inicializace se vstupuje na stav blocking, z blocking stavu na stav listening, z listening stavu na stav learning a z learning stavu to končí na stavu forwarding. Z forwarding se může přejít na stav disabled, ovšem není to nutností, je to pouze jednou z možností. [10]



Obrázek 5 - Stavový diagram STP protokolu

Přepracováno od zdroje: Spanning Tree Protocols – Cisco [23]

2.2 Role portů u STP protokolu

Kromě toho, že má každý port na switch zařízení, které využívá STP protokol vždy svůj určitý stav, tak má i zároveň každý port na switch zařízení svoji roli. Podle role konkrétního portu se určuje, jakým způsobem se daný port bude podílet při procesu STP protokolu. Z tohoto důvodu jsou definovány následující tři role pro porty:

- **Root port** – Jedná se o port, který má nejkratší cestu, tedy nejnižší hodnotu Cost k Root Bridge zařízení. Tento port se neobjevuje na root bridge zařízení, kdežto na ostatních zařízeních stejného typu se nachází přímo jeden root port. Root port přijímá rámce a předává je do root bridge zařízení. [22; 31; 33]
- **Designated port** – Jedná se o port, který přesměrovává síťový provoz směrem ven ze strany root bridge zařízení. Jak už bylo zmíněno výše, tak root bridge zařízení neobsahuje root porty, ale obsahuje právě tyto porty, odborně zvané jako designated porty. Designated port má v určitém segmentu nejkratší cestu k root portu. Designated bridge zařízení má pro každý spoj právě jeden designated port. [22; 31; 32; 33]
- **Non-designated port** – Jedná se o port, který při STP protokolu nedostal definovanou roli ani jako root port ani jako designated port. Znamená to tedy, že se jedná o blokovaný port. Takovému portu je tedy blokováno směrování v průběhu

síťového provozu. Tyto porty i přesto zůstávají stále zapnuté a slouží jako záloha v případě, kdyby mělo dojít k výpadku u hlavní cesty pro směrování. [31; 32; 33]

2.3 Časovače STP protokolu

K tomu, aby se zajistilo, zda je konkrétní síťová topologie při STP protokolu stabilní a jestli se duplicitní rámce nedostaly do sítě před zahájením procesu směrování, se používají časovače tzv. Spanning Tree timers, které jsou obsažené v jednotce BPDU.

- **Hello** – V případě typu Hello, se jedná o čas mezi každou jednotkou BPDU, která je odeslána na konkrétní port. Hodnota tohoto času se ve výchozím stavu rovná dvou sekundám. Tato hodnota je nastavitelná, tudíž je možné jí měnit v rozmezí jedné až deseti sekund.
- **Forward delay** – Forward delay je časová hodnota, která se odráží od doby odpovídající pobytu ve stavu listening a ve stavu learning. Hodnota tohoto času se ve výchozím stavu rovná patnácti sekundám. Tato hodnota je taktéž nastavitelná, tudíž je možné jí také měnit, a to v rozmezí čtyř až třiceti sekund.
- **Max age** – Časovač typu Max age řídí maximální délku časové hodnoty, která uplyne dříve, než bridge port uloží veškeré konfigurační informace BPDU jednotky. Hodnota tohoto času se ve výchozím stavu rovná dvaceti sekundám. Tato hodnota je stejně jako předchozí zmíněné hodnoty nastavitelná, tudíž je možné jí také měnit, a to v rozmezí šesti až čtyřiceti sekund.

  [10]

2.4 Nevýhody STP protokolu

STP protokol je při nasazení v sítích na linkové vrstvě (L2) v mnoha ohledech užitečný, ovšem nic není dokonalé, a dokonce i ve STP protokolu se vyskytují jisté nedostatky, těmi konkrétně jsou:

- Původní verze STP protokolu, u které je nezbytné udržovat kompatibilitu s vyvíjejícími verzemi, disponuje charakterem typu „fail-open“. To znamená, že při poruše se může vyskytnout nevyžádaná chybová situace, ve které se hlavní i zbylé záložní spoje aktivují souběžně a způsobí to zahlcení sítě.
- Jedinou použitelnou logickou topologií pro síť založenou na switch zařízeních je stromová topologie. Stromová topologie nese jisté omezení na návrh počítačové sítě. To omezení je takové, že části stromové topologie je

potřeba navrhnout a nakonfigurovat manuálně. Zároveň je nezbytné, aby byla důkladně promyšlená implementace pro ochranné prostředky.

- Jak už bylo zmíněno výše, že nic není dokonalé, tak i stabilita sítě není dokonalá a následné dohledávání zdrojů nestability není úplně jednoduchou záležitostí. Pokud dojde k zahlcení sítě, není už možné provést analýzu zachovalými postupy. Nejsou zde k dispozici pomocné nástroje jako je „traceroute“ nebo „ping“, které zrovna u TRILL protokolu možné jsou.
- Velká část spojů, v oblasti distribuční vrstvy a v oblasti vrstvy páteřní, bývá blokována a nedochází tak k jejich využití, z čehož vyplývá, že dochází k mrhání jejich přenosové kapacity.

[4]

2.5 Další varianty STP protokolu

STP protokol se neustále vyvíjel a přicházely na svět jeho modifikované verze, kterými byly konkrétně RSTP, MSTP a PVST.

2.5.1 RSTP protokol

RSTP neboli Rapid Spanning Tree Protocol, který spadá pod standard IEEE 802.1w, je pokrokovým protokolem pro původní Spanning Tree Protocol (STP), spadající pod standard IEEE 802.1d. RSTP protokol podporuje vysokou dostupnost a také topologii charakteru „loop-free“ v rámci sítí typu Ethernet. [42]

Zásadní výhodou navrhnutých sítí, které disponují RSTP protokolem je, že nabízejí rychlejší konvergenci při změně topologie sítě ve srovnání s tradiční topologií sběrnicového zapojení. V případě, kdy dojde k selhání sítě, tak zařízení mohou i přesto pokračovat v komunikaci skrz danou počítačovou síť, protože potřebná data lze přesměrovat, při výskytu síťového selhání. [42]

RSTP protokol systematicky zabraňuje síťovým smyčkám při využití většího počtu switch zařízení metodou blokování redundantních cest v počítačové síti. RSTP protokol je ve své podstatě jistým souhrnem pravidel, podle kterých switch zařízení v dané počítačové síti určují nejvíce ideální způsob pro odeslání vysílání typu broadcast skrz síť, kde se ustanoví root bridge zařízení a blokují se konkrétní porty, a to všechno za účelem prevence síťových smyček. [42]

2.5.1.1 Změny RSTP protokolu oproti STP protokolu

- Upravený formát BPDU jednotky, v RSTP protokolu se používá verze 2.
- V původním STP protokolu byly tři role pro porty. RSTP protokol disponuje čtyřmi rolemi pro porty a těmi jsou root role, designated role, backup role a alternate role.

- Změnil se také počet stavů pro porty, kde v případě STP protokolu jich je pět a v případě RSTP protokolu jsou pouze tři. Jsou to stavy Forwarding, Learning a stav Discarding.
- Místo přeposílání Root BPDU jednotky, jako tomu bylo u STP protokolu, tak u RSTP protokolu všechna switch zařízení umí generovat BPDU jednotky, které jsou zde posílány na všechny porty při každém časovém úseku typu Hello time.
- Posílají se zde jednotky BPDU typu Agreement / Proposal.
- Pro konkrétní síťové spoje jsou definovány jejich typy, kterými jsou například point-to-point, edge či shared, což znamená, že některé z nich mohou přejít rychlým tempem do stavu Forwarding.
  [25]

2.5.1.2 Role portů u RSTP protokolu

Jak už bylo zmíněno v předchozí podkapitole, tak u RSTP protokolu se oproti STP protokolu zvýšil počet rolí pro konkrétní porty. Místo třech, jako tomu bylo původně, jsou zde u RSTP protokolu čtyři typy rolí. Zůstávají zde role typu root port a designated port. Ovšem není už zde role non-designated port. Nově nabytými rolemi portů jsou role Alternate port a role Backup port.

- **Alternate port** – Jedná se o port, který poskytuje alternativní cestu k root bridgi pro případ, že dojde k situaci, kdy se root port dopustí výpadku a umístí se tak do stavu Discarding. Tento port není součástí aktivního procesu činnosti RSTP protokolu, ale jakmile root port selže, tak alternate port okamžitě převezme kontrolu nad procesem. [22]
- **Backup port** – Jedná se o port, který poskytuje záložní cestu k částem procesu RSTP protokolu pro případ, že dojde k situaci, kdy se designated port dopustí výpadku a umístí se tak do stavu Discarding. Backup port může existovat pouze na místech, kde se dva nebo tři další porty pro bridge připojují do stejné počítačové sítě typu LAN, pro kterou bridge funguje v roli jako designated bridge. Jakmile designated port selže, tak backup port okamžitě převezme kontrolu nad procesem. [22]

2.5.1.3 Stavy portů u RSTP protokolu

Jak už bylo zmíněno výše, že se u RSTP protokolu oproti STP protokolu změnil počet rolí portů, tak se i zároveň ve srovnání s STP protokolem změnil počet stavů pro porty. Ovšem v případě stavů nedošlo o zvýšení počtu, ale naopak právě o snížení počtu z pěti stavů pouze na tři stavy. Těmi zmíněnými stavy jsou:

- **Discarding** – Jedná se o stav při RSTP protokolu, který kombinuje tři stavy z STP protokolu, což jsou stavy Diabled, Blocking a Listening. Ve stavu Discarding, port vyřadí veškeré přijaté rámce a neodchází zde k učení MAC adres. [22; 31; 32]
- **Learning** – Jedná se o stav, kde se port připravuje na směrování po síťovém provozu takovým způsobem, že zkoumá přijaté rámce pro informace o poloze za účelem vytvoření tabulky MAC adres. Proto zde už dochází k učení MAC adres. Tento stav v podstatě funguje téměř stejně jako v případě STP protokolu. [22; 31; 32]
- **Forwarding** – Jedná se o stav, kde port filtruje rámce a následně je směruje dále. Konkrétní port v tomto stavu je aktivní součástí procesu činnosti RSTP protokolu. Opět tento stav v podstatě funguje téměř stejně jako v případě STP protokolu. [22; 31; 32]

2.5.2 MSTP protokol

MSTP neboli Multiple Spanning Tree Protocol vznikl jako rozšíření pro RSTP protokol, byl definován ve standardu IEEE 802.1s, ovšem později, konkrétně v roce 2003 byl začleněn do standardu IEEE 802.1q. Standard IEEE 802.1q popisuje sítě typu VLAN. MSTP protokol se sítěmi typu VLAN, přímo souvisí. Jako základ se používá RSTP protokol, ale navíc je možné seskupovat sítě typu VLAN do instancí typu spanning-tree. To znamená, že pro každou vytvořenou skupinu běží samostatná instance STP protokolu. Za pomocí toho je možné využít více cest pro směrování a také je možné provádět jednoduchý proces load balancingu. Obvykle MSTP protokol umožňuje vytvořit až šedesátpět odlišných logických topologií či instancí. [25]

MSTP protokol disponuje skupinou switch zařízení, které mají stejnou konfiguraci, to znamená, že mají stejným způsobem mapované instance na VLAN sítě. Této skupině switch zařízení se odborně říká MST region. Jednotlivé regiony či switch zařízení, která nemají implementovaný MSTP protokol, jsou společně propojeny klasickým nemodifikovaným STP protokolem. To znamená, že aby se konkrétní switch stal součástí regionu a měl by tedy i spoluúčast u MSTP protokolu, musí mít z takového důvodu stejnou konfiguraci jako ostatní switche v dané skupině. To znamená, že musí být stejné jméno regionu, stejné číslo revize a stejné mapování VLAN na instance. [25]

MST instance prezentuje mapování VLAN do jednotlivých skupin. V jednom regionu lze vytvořit řadu instancí se skupinami VLAN sítí, rozsah čísel je od nuly až do hodnoty 4094 (2^12 – 2), ovšem maximálně může být šedesátpět instancí. Defaultně jsou všechny VLAN sítě začleněné do instance nula, tedy MST00. [25]

V případě přechodu na MSTP protokol či změně začlenění VLAN sítě do MST instance dojde znovu k inicializaci a tudíž i ke dočasnému výpadku spojení. [25]

2.5.3 PVST protokol

PVST, někdy značený i zkratkou PVSTP či konkrétně Per-VLAN Spanning Tree, je Cisco proprietární protokol typu STP, který provozuje samostatnou instanci STP protokolu pro každou jednotlivou VLAN. Samostatná instance protokolu STP pro každou VLAN podsíť pomáhá ke konfiguraci VLAN nezávislým způsobem, což také pomáhá rovněž k výkonu. Per-VLAN Spanning Tree (PVST) protokol pro svou funkci vyžaduje Inter-Switch Link (ISL) protokol. [31; 33; 34]

Pro PVST protokol existuje rozšíření PVST+, které umožňuje interoperabilitu mezi CST a PVST ve switch zařízeních od společnosti Cisco a podporuje standard IEEE 802.1Q. [48]

3 Podobná řešení TRILL protokolu

TRILL protokol nebyl zcela jediným řešením, který měl nahradit STP (Spanning Tree Protocol). Jedním téměř stejným řešením je FabricPath od společnosti Cisco. Druhým řešením je technologie spadající pod síťový standard IEEE 802.1aq a tou je SPB neboli Shortest Path Bridging.

3.1 Cisco FabricPath

Řešení FabricPath bylo představené společností Cisco v síťovém operačním systému pro switche, kterým byl Nexus OS, a to ve verzi 5.1. Cisco FabricPath umožňuje pro návrh sítě realizovat vysoce škálovatelné topologie druhé vrstvy (L2) referenčního modelu ISO/OSI. FabricPath umožňuje realizovat nasazení typu plug and play s tím, že umí využít výhody třetí síťové vrstvy (L3), které poskytují počítačovým sítím s nasazením FabricPath, možnost škálovat s nesrovnatelnou úrovni oproti sítím využívající pouze STP protokol. Díky své jednoduchosti umožňuje FabricPath rychlejší a jednodušší sítě datových center. [53]

Jelikož používá jiné záhlaví u rámců, než jaké používá TRILL protokol, tak z toho důvodu s ním není kompatibilní.

3.2 Shortest Path Bridging (SPB)

SPB neboli Shortest Path Bridging je technologie spadající pro síťový standard IEEE 802.1aq, jehož původním cílem bylo nahradit STP (Spanning Tree Protocol) protokol stejně jako tomu bylo u TRILL protokolu. SPB umožňuje služby VPN podobné multiprotokolovému přepojování (MPLS), ovšem jeho údržba a nasazení je značně jednodušší. Na rozdíl od MPLS metody, která vyžaduje větší množství protokolů, kterými jsou například OSPF, MP-BGP, LDP, RSVP a další, tak SPB při poskytování této funkce využívá pouze jeden jediný protokol a tím je link state routing protokol IS-IS. IS-IS, neboli Intermediate System to Intermediate System, je jediným protokolem řídicí vrstvy, který je nezbytně nutný k vytvoření topologie sítě s více cestami (tzv. multi-path) k učení adres a k přenesení VPN tras přes backbone. [27]

Za pomocí link state routing protokolu IS-IS a MAC-in-MAC zapouzdření vytváří SPB technologie libovolnou, škálovatelnou a rychle konvergující strukturu, která podporuje více aktivních optimálních cest pro routovací provoz a pro provoz bridgů. [27]

V rámci SPB existují dva typy modelů pro vícecestné bridging směrování, jedním z nich je Shortest Path Bridging VLAN (SPBV) a tím druhým je Shortest Path Bridging Mac-in-Mac (SPBM). Obě tyto varianty používají link state routing protokol IS-IS v rámci topologie a oba mají za úkol za pomocí algoritmu vypočítat nejkratší cesty mezi zařízeními. SPBV k určení dosažitelnosti jednotlivých uzlů v síti používá hodnotu Shortest Path VLAN ID (SPVID). Kdežto SPBM k určení dosažitelnosti jednotlivých uzlů v síti používá kombinaci hodnot Backbone VLAN ID (BVID) a Backbone MAC (BMAC). Obě varianty SPBV i SPBM jsou schopné si poskytovat služby a spolupracovat s STP protokolem. [26]

Následující tabulka č. 1 znázorňuje porovnání technologie SPB s TRILL protokolem v mnoha bodech.

	TRILL	SPB
Standard	IETF	IEEE 802.1aq
Spolupráce s STP protokolem	Ano	Ano
Náhrada za STP protokol	Ano	Ano
Podpora multi-pathingu	Ano	Ano
Podpora virtualizace	4096 VLAN (bez dodatečného rozšíření)	16 milionů VLAN
Typ zapouzdření pro rámce	TRILL záhlaví (TRILL header)	MAC-in-MAC (pro SPBM) a Q-in-Q (pro SPBV)
Hodnota TTL v záhlaví rámce	Ano	Ne
Možnost využití pingu	Ano	Ne
Možnost využití traceroute	Ano	Ne
Využití IS-IS protkolu	Ano	Ano
Volba při procesech	Root Bridge, Designated RBridge, nickname hodnoty u RBridge zařízení	Předem zajištěná
Nutná úprava záhlaví u každého prvku	Ano	Ne
Cesta v síťovém provozu pro Unicast	Nejkratší cesta na základě výpočtů IS-IS protokolu	Nejkratší cesta na základě výpočtů IS-IS protokolu
Cesta v síťovém provozu pro Multicast či Broadcast	Závisí na zvoleném Root Bridge	Mezi dvěma koncovými síťovými prvky, obousměrně shodnými na základě zdrojového síťového zařízení
Škálovatelnost	Větší než 10 000	Větší než 10 000 s rozšířením IS-IS protkolu
Dynamické změny síťových cest pro směrování v síťovém provozu	Ano	Ano
Výstupní zpracování pro	Je vyžadováno, z důvodu změny záhlaví MAC adresy	Není potřeba

Multicast	na výstupním portu	
Učení MAC adres (MAC Learning)	Pomocí protokolu ESADI	Na základě síťové jednotky na kraji SPB sítě
Potřeba nového hardwarového vybavení pro implementaci protokolu	Ano, z důvodu záhlaví TRILL protokolu	Ve většině případů to nutné není, jelikož mnoho switch zařízení umí fungovat s metodami MAC-in-MAC a Q-in-Q
Možnost implementace nových síťových prvků do existující sítě	Může být, jak z okrajů sítě, tak i z jejího jádra	Pouze z oblasti jádra sítě
Doplnění IS-IS protokolu	Upraven s novou jednotkou PDU	Rozšířen s TLV
Odolnost vůči smyčkám	Vysoká	Střední
Prevence proti smyčkám	RPFC a na základě hodnoty hop count u TTL	RPFC
Forwarding a Lookup	Využití MAC swapování; Frame Check Sequance	Podobné jako u sítě typu Ethernet; v rámci uzlů BCB a BEB; není využito MAC swapování
Agregace služeb	Ne	Ano
Konvergence	Každý port oznamuje všechny VLAN sítě, skrz Hello rámec; na 1 port může být posláno až 4096 oznámení typu Hello	Odvíjí se od zdrojového síťového prvku, na základě výpočtu ze stromových struktur, počet stromů vychází z počtu síťových uzlů
Správa síťového provozu	Přiřadí se nejkratší cesta pro Unicast vysílání se záhlavím linkové vrstvy (L2) na každém RBridge zařízení v síti; spoje se odvíjí od hodnot metrik pro výpočty možných cest	Provoz se přiřadí k nejkratším cestám; spoje se odvíjí od hodnot metrik pro výpočty možných cest
Zjednodušení Troubleshootingu	Je zapotřebí kontrolovat síťový provoz na principu hop-by-hop, aby byla znát celá cesta; OAM nástroje	U SPB je skrz síť vidět celá cesta; OAM nástroje jsou k dispozici

	nejsou k dispozici	
Možnost zkombinovat výhody obou protokolů	TRILL protokol může společně existovat s metodou Q-in-Q a také může využít dostupnost škálovatelnosti VLAN identifikátorů	SPB neumí fungovat s pokročilejšími vlastnostmi síťové vrstvy (L3)
Využití v sítích typů	Datová centra, později i u poskytovatelů služeb (Service Providers)	Poskytovatelé služeb (Service Providers)
Systémové ID	Potenciální kolize nicknamů, v průběhu připojování do sítě s TRILL protokolem (TRILL network)	Názvy síťových uzlů využívají ustanovené systémové ID hodnoty

Tabulka 1- porovnání TRILL protokolu a SPB

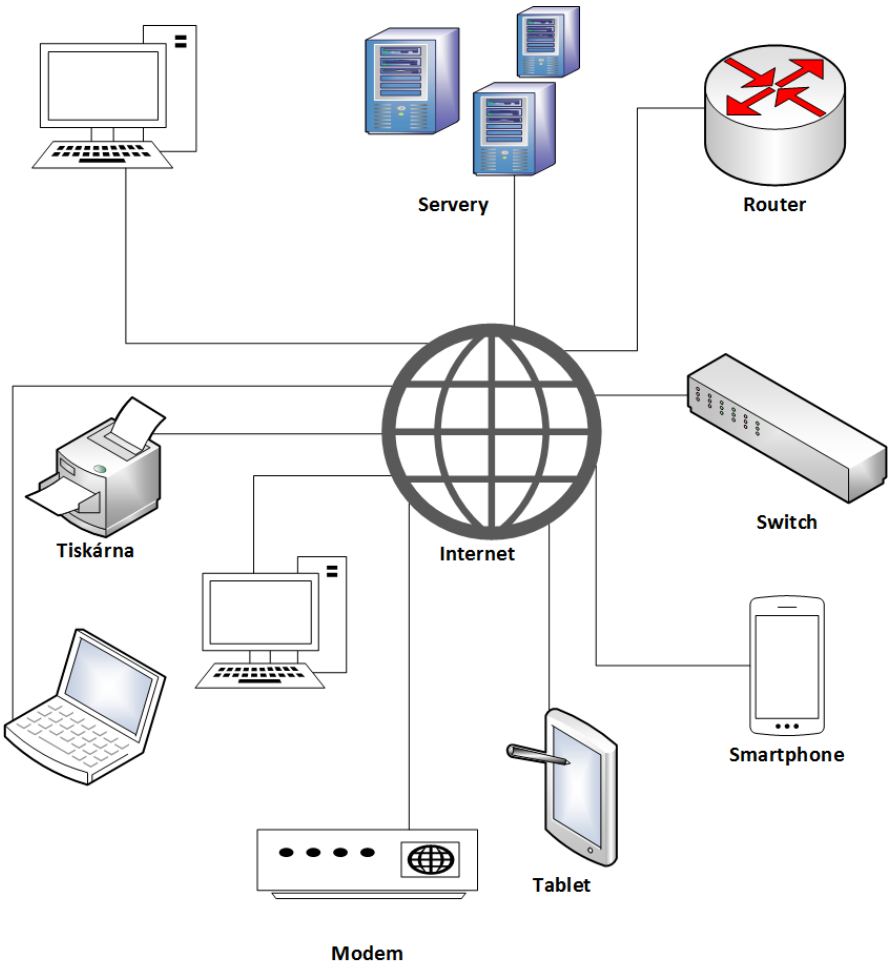
Přepracováno od zdrojů: Ing. Miroslav Matuška, Ph.D - TRILL 4. část – Stav vývoje a alternativní řešení; Compare and Contrast SPB and TRILL – Avaya; Mikael Holmberg – TRILL vs. SPB [14; 26; 28]

Jelikož si technologie TRILL a Cisco FabricPath jsou velice podobné svými výhodami, tak z tohoto důvodu došlo k důkladném porovnání pouze s technologií SPB.

4 Počítačová síť

Počítačová síť je jeden velký svět, který můžeme vnímat z více úhlů pohledu. Obecně lze počítačovou síť definovat jako propojení mezi více zařízeními, která jsou vzájemně propojená tak, aby mezi nimi fungovala komunikace. Může se jednat o zařízení jako jsou počítače, notebooky, mobilní telefony, tiskárny nebo například i chytré hodinky. V počítačové síti figurují síťové prvky, které se dělí na dvě skupiny a těmi jsou aktivní síťové prvky a pasivní síťové prvky. Mezi aktivní síťové prvky patří například router (směrovač), switch, hub, repeater, bridge či třeba access point. Mezi pasivní síťové prvky patří například veškerá kabeláž, spojky, konektory, zásuvky či třeba všechna přenosová media. Počítačové sítě lze dělit mnoha způsoby, nejčastějším způsobem pro členění typů počítačových sítí je však dělení dle rozsahu. Nejznámějšími typy síti, které jsou kategorizované dle rozsahu jsou PAN (Personal Area Network), MAN (Metropolitan Area Network), LAN (Local Area Network) a WAN (Wide Area Network). Existují ještě méně populární typy sítí kategorizované dle rozsahu a těmi jsou CAN (Campus Area Network) a GAN (Global Area Network). Pro příklad řešení komunikace v oblasti počítačových a telekomunikačních sítí se používá referenční model ISO/OSI.

Obrázek č. 6 znázorňuje zjednodušené schéma obecné počítačové sítě.



Obrázek 6 - Schéma počítačové sítě

LAN neboli Local Area Network jsou zřejmě nejpoužívanějším typem sítí dle rozsahu. Jsou určené speciálně pro lokální zavedení, v rozsahu přibližně několika desítek či stovek metrů. Využívají se převážně v podnicích, školách a zároveň i v domácnostech. Hodnoty přenosových rychlostí se pohybují v jednotkách Gb/s. Nejpoužívanějšími technologiemi pro sítě typu LAN jsou Ethernet a Wi-Fi. Nejčastěji se používají pro sdílení internetového připojení a sdílení prostoru na disku, ovšem mají i využití jinde. Na tento typ počítačových sítí je zaměřena simulace podnikové sítě pro nasazení TRILL protokolu. [39]

PAN neboli Personal Area Network jsou v rámci rozsahu těmi nejmenšími sítěmi, jedná se o sítě osobní. Pod těmito sítěmi si lze představit například propojení osobního počítače, notebooku, tabletu, chytrého mobilního telefonu či třeba i chytrých hodinek do sítě, která je v blízkosti jedné osoby, což v praxi znamená do vzdálenosti pouze několika metrů. Tato síťová spojení mohou být v případě jedné možnosti drátová, například prostřednictvím USB kabelu nebo při druhé aktuálně častější možnosti mohou být tato síťová spojení bezdrátová, a to prostřednictvím Wi-Fi sítě či Bluetooth spárování. [39]

CAN neboli Campus Area Network jsou převážně zavedené pro univerzitní sítě, jedná se zároveň o speciální typ sítí typu MAN (Metropolitan Area Network), který je ve většině případů omezený na specifické oblasti v rámci školy či kampusu. CAN síť a celé její vybavení, bývá v nejvíce případech vlastněné na straně univerzity či organizace. Počítačové sítě typu CAN nemusí být využité pouze v rámci univerzit. Lze je také využít v oblasti rozsáhlejších firem. Hodnoty přenosové rychlosti se v počítačových sítích typu CAN pohybují v jednotkách Gb/s. [39]

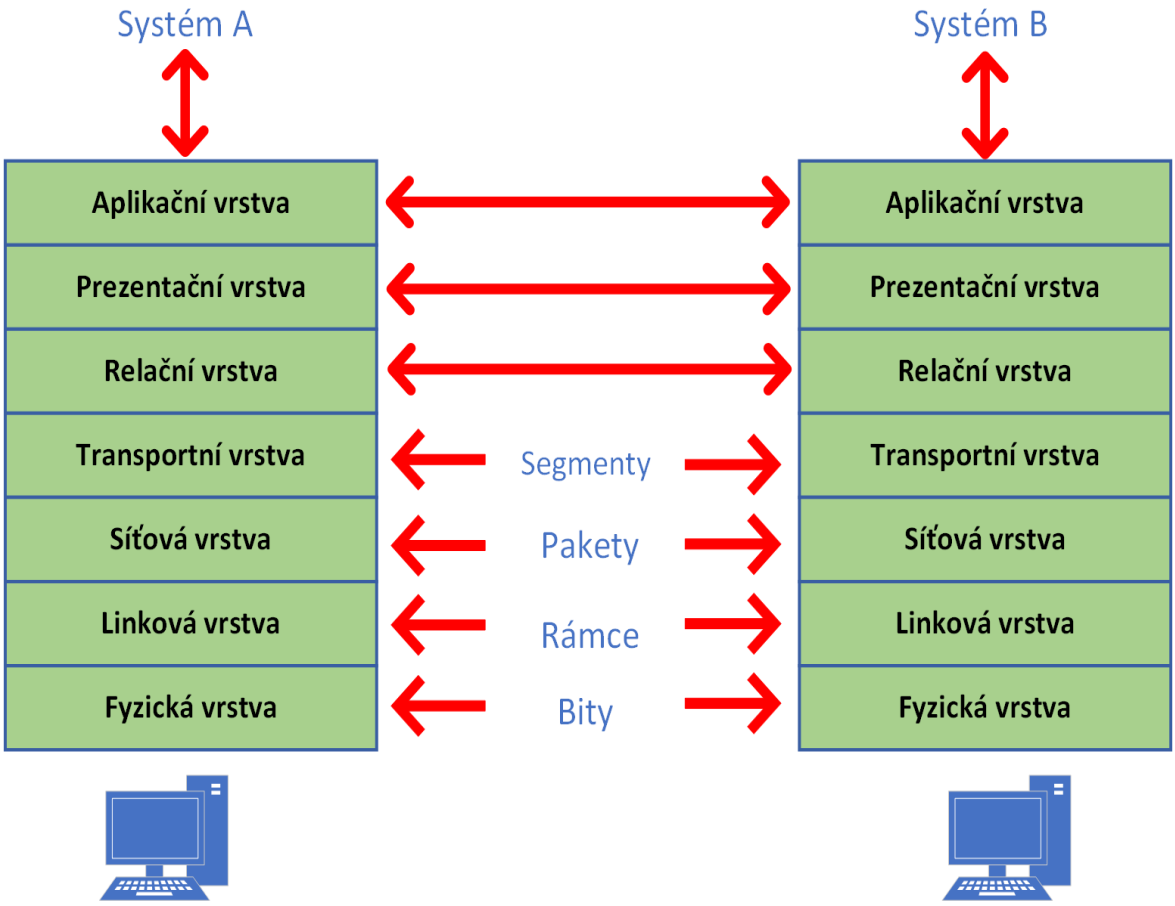
MAN neboli Metropolitan Area Network jsou typem sítí, které jsou jakýmsi prostředníkem mezi počítačovými sítěmi typu LAN a WAN. Jedná se o počítačové sítě rozsahu města. Jelikož počítačové sítě typu MAN, vyžadují velké hodnoty přenosových rychlostí, tak se z takového důvodu pro ně často využívají optické kabely či mikrovlnné spoje. Z pohledu topologie počítačových sítí jsou metropolitní sítě většinou typu backbone. Hodnoty přenosových rychlostí se v počítačových sítích typu MAN pohybují v řádech Mb/s. [39]

GAN neboli Global Area Network je typem sítě, která je globální, jak už její název říká. Jedná se o nejrozsáhlejší síť, a to hlavně za pomoci využití bezdrátových technologií a satelitů, čímž se ve své podstatě stává neomezenou sítí. Základní přenosové rychlosti počítačových sítí typu GAN se pohybují v řádech Mb/s. Příkladem sítě typu GAN je Internet. [39]

WAN neboli Wide Area Network je typem rozlehlé počítačové sítě, která je podobná síti typu GAN, ovšem nedosahuje takového charakteru. Počítačová síť typu WAN bývá často označována jako spojení několika sítí typu LAN do jednoho celku. Počítačové sítě typu WAN se v nejvíce případech aplikují způsoby pronajatými linkami, přepojováním paketů, přepojováním buněk nebo přepojováním okruhů. [39]

4.1 Referenční model ISO/OSI

Referenční model ISO/OSI se skládá ze sedmi vrstev, z entit a z protokolů a služeb. Každá vrstva modelu ISO/OSI odpovídá nějaké konkrétní funkci. Téměř všechny vrstvy přiléhají k určité vrstvě z obou stran, a to jak k té nižší, tak i k té vyšší. Jinak tomu je v případě sedmé aplikační vrstvy (L7), tedy té nejvyšší, ta přiléhá přímo aplikačnímu procesu. Jinak tomu je také, v případě první fyzické vrstvy (L1), tedy té nejnižší, která sdílí rozhraní přímo s fyzickým zařízením. Entita je objekt, který v určité vrstvě vykonává příslušnou činnost. Entity ve svých příslušných vrstvách, pro komunikaci mezi sebou využívají jistá pravidla, kterými jsou protokoly. [39]



Obrázek 7 - Referenční model ISO OSI

Přepracováno od zdroje: Libor Dostálek a Alena Kabelová - Velký průvodce protokoly TCP/IP a systémem DNS [40]

4.1.1 Fyzická vrstva

Fyzická vrstva, tedy první vrstva (L1) referenčního modelu ISO/OSI, se týká elektrických či optických signálů používaných při komunikaci mezi elektronickými zařízeními. Na fyzické vrstvě (L1) je zaveden fyzický okruh. Na fyzickém okruhu mezi dvě elektronická zařízení bývají často dodatečně vkládána další elektronická zařízení, kterými můžou být například modemy. [40]

Úkolem fyzické vrstvy (L1) je obstarat přenos jednotlivých bitů mezi stranou příjemce a stranou odesílatele, za pomocí fyzické přenosové cesty, kterou fyzická vrstva umí ovládat. [58]

4.1.2 Linková vrstva

Linková vrstva, tedy druhá vrstva (L2) referenčního modelu ISO/OSI zajišťuje v případě zapojení sériových linek výměnu dat mezi sousedními elektronickými zařízeními a v případě sítí typu LAN, jde o výměnu dat v uvnitř dané lokální sítě. Na linkové vrstvě (L2) slouží pro přenos dat, základní síťová jednotka, které se říká datový rámec. Datový rámec má tři hlavní části, mezi které patří záhlaví, přenášená data neboli payload a poslední částí je zápatí. [40]

Datový rámec obsahuje ve svém záhlaví linkovou adresu odesílatele, linkovou adresu příjemce a další potřebné informace. V zápatí datového rámce, bývá obvykle kontrolní redundantní součet (CRC) z přenášených dat. Za pomocí kontrolního redundantního součtu (CRC) lze zjistit, jestli se například při přenosu nepřihodilo porušení dat. [40]

Linková vrstva, pro stranu odesílatele potvrzuje případné přijetí nepoškozeně přenesených rámců. Ovšem, pokud odesílateli přijdou rámce poškozené, tak si linková vrstva vyžádá jejich zpětné zaslání.[58]

4.1.3 Síťová vrstva

Síťová vrstva, tedy třetí vrstva (L3) referenčního modelu ISO/OSI, slouží k zabezpečení přenosu dat mezi vzdálenými elektronickými zařízeními, v síti typu WAN. Na síťové vrstvě (L3) slouží k přenosu síťová jednotka, které se říká síťový paket. Síťový paket je balen do datového rámce. Síťový paket se většinou skládá pouze ze záhlaví a datového pole. [40]

4.1.4 Transportní vrstva

Transportní vrstva, tedy čtvrtá vrstva (L4) referenčního modelu ISO/OSI má od třetí síťové vrstvy (L3) k dispozici její služby, které jí zajišťují přenos síťových paketů mezi dvěma libovolnými koncovými zařízeními v počítačové síti. [58]

Při odesílání dat má transportní vrstva (L4) na starost skládání jednotlivých paketů, do kterých jsou tříděné přenášená data. Když dojde k přijetí, tak jsou data z paketů vyjmuta a následně se složí do původního tvaru. Takovým způsobem je možné zajistit přenos zpráv s libovolnou velikostí i přesto, že jednotlivé pakety jsou limitovány svojí velikostí. [58]

Na transportní vrstvě (L4) slouží k přenosu síťová jednotka, které se říká transportní paket nebo také bývá někdy nazývána i jako datagram. Transportní paket se skládá ze záhlaví a datové části a přenáší se v datové části síťového paketu. [40]

Nejznámějšími protokoly transportní vrstvy jsou protokoly TCP a UDP.

4.1.5 Relační vrstva

Relační vrstva, tedy pátá vrstva (L5) referenčního modelu ISO/OSI se stará o zabezpečení výměny dat mezi aplikacemi. Jejím úkolem je navazování, udržování a případné rušení relací neboli sessions mezi koncovými klienty. Na základě navazování relace si relační vrstva (L5) vyžádá od vrstvy transportní možnost pro vytvoření spojení, skrz které následně probíhá komunikace mezi oběma stranami dané relace. [40; 58]

Základní síťovou jednotkou v relační vrstvě (L5) je relační paket, který je klasicky vkládán do paketu transportní vrstvy. [40]

4.1.6 Prezentační vrstva

Prezentační vrstva, tedy šestá vrstva (L6) referenčního modelu ISO/OSI nese zodpovědnost za reprezentaci a zabezpečení dat. Reprezentace dat se může na různých koncových zařízeních významně lišit. V případě zabezpečení je zde řeč o zabezpečení integrity dat, šifrování či digitálního podepisování. [40]

4.1.7 Aplikační vrstva

Aplikační vrstva, tedy sedmá vrstva (L7) referenčního modelu ISO/OSI má za úkol poskytovat služby pro aplikace. Aplikační vrstva předurčuje, v jakém formátu a jakým způsobem mají být určitá data vyhotovena od aplikačních programů. V aplikační vrstvě se například nachází souborové servery, tiskové servery, programy pro řízení databází a příkazy operačního systému. Jedná se o jedinou vrstvu referenčního modelu ISO/OSI, do které má uživatel přístup. [39; 40]

Mezi protokoly aplikační vrstvy patří například DHCP, FTP, SMTP, POP3, SSH a mnohé další.

5 VLAN

VLAN neboli Virtual Area Network je typem virtuální sítě, která slouží k logickému rozdělení existující sítě, bez ohledu na uspořádání fyzických zařízení. Síť se tedy může rozdělovat na menší sítě, z vnitřní části fyzické struktury původní počítačové sítě. Za pomocí sítě typu VLAN, je možné dosáhnout stejného účinku, jako když je k dispozici skupina fyzických síťových zařízení, připojených do jednoho či několika propojených switchů a druhou skupinu do jiných switch zařízení. Jedná se o dvě na sobě nezávislé sítě, které spolu nemohou komunikovat, z důvodu jejich fyzického rozdělení. Pomocí VLAN technologie je možné takové dvě sítě vytvořit na jednom či klidně na několika propojených switch zařízeních. [44]

5.1 Důvod vzniku sítí typu VLAN

Důvodů, proč byly zavedeny sítě typu VLAN může být mnoho, těmi hlavními ovšem byly:

- Snížení oběžníků (broadcastů) v počítačových sítí
- Zmenšení kolizních domén v době, kdy se nepoužívaly switche, ale zařízení první vrstvy referenčního modelu ISO/OSI, tedy huby
- Shromažďování uživatelů v počítačové síti, na základě skupin či podle služeb, místo podle fyzického umístění a oddělení komunikace mezi těmito skupinami [44]

5.2 Výhody VLAN sítí

Mezi praktické výhody VLAN sítí patří primárně:

- Jednou z výhod je snížení počtu potřebného hardwarového vybavení, to ovšem neznamená, že se snižuje potřebný počet portů. Tím, že mohou být různé podsítě na stejném switch zařízení, je možné je lépe využít, například pro propojení tří zařízení není potřeba žádný speciální switch, který má minimálně 8 portů.
- Zvýšení zabezpečení z důvodu oddělené komunikace do speciální VLAN části, do které není jiný přístup. Toho je možné dosáhnout použitím samostatných switchů.
- Jak už bylo zmíněno v předchozí podkapitole, tak značnou výhodou VLAN je snížení oběžníků (broadcastů). Výhodou je vytvoření většího počtu broadcastových domén, které jsou menší. To pomáhá, ke zlepšení výkonu sítě snížením jejího provozu.
- Zjednodušená správa u sítí, a to takovým způsobem, že při přesunu jednoho zařízení do jiné sítě stačí pouze upravit konfiguraci zařazení do VLAN sítě, tedy prověřená osoba, konfiguruje software, konkrétně zařazení do VLAN sítě, a ne hardwarové vybavení.

- Oddělení speciálního provozu, jelikož dnes se používá řada provozu, který nemusí být propojen kompletní časti sítě, ale přesto je potřeba ho dostat na různá místa, navíc není vhodné, aby ovlivňoval běžný provoz.
  [44]

5.3 Zařazení komunikace do VLAN

Přiřazení do VLAN sítě, probíhá nastavením typickým způsobem na switch zařízeních, pouze v ojedinělých případech přichází označená komunikace přes trunk z jiného zařízení. Trunk je port, který je zařazen do více VLAN sítí. Na switchích, které podporují VLAN sítě, vždy existuje minimálně jedna VLAN síť. Řeč je v takovém případě o defaultním VLAN číslu 1, které není možné žádným způsobem vymazat či vypnout. V případě, kdy nedojde ke speciálnímu nastavení, tak je zvykem, že jsou všechny porty, tedy veškerá komunikace zařazené do VLAN 1. [44]

Pro zařazení komunikace do VLAN sítě, existují čtyři základní metody. Jednou z metod je zařazení podle portu, dalšími metodami jsou zařazení podle autentizace, zařazení podle MAC adresy a zařazení podle protokolu. V praxi se nejčastěji využívá možnost pro zařazení podle portu. [44]

5.4 Typy VLAN sítí

VLAN sítě se podle značení dělí na dva typy, kterými jsou tagovaná VLAN a netagovaná VLAN.

Tagovaná VLAN je taková, kde každý port switche může přenášet více tagovaných VLAN, na protějším zařízení musí být nastavena stejná norma a zařízení musí pakety či rámce tagovat. Každý paket či rámec, procházející takovým portem obsahuje tag, aby switch věděl příslušnost daného paketu či rámce k dané VLAN síti. Pokud paket či rámec nemá tag, tak je v takovém případě zahozen nebo může být dle nastavení portu zařazen do netagované VLAN sítě. [52]

Netagovaná VLAN je taková, kde každý port switche může být pouze v jedné netagované VLAN síti, na protějším zařízení se nemusí nastavovat žádné přiřazení do VLAN sítě. Pokud příchozí paket či rámec nemá žádný VLAN tag, automaticky dostává tag dle nastavení konkrétního portu. Netagovaná VLAN síť se zadává ve switchi pomocí hodnoty PVID (Port Vlan ID), což je označení, do které lze VLAN netagované pakety či rámce tagovat. [52]

5.5 Typy portů u VLAN sítí

U VLAN sítí existují tři typy portů, kterými jsou trunk port, port přístupový (tedy access port) a hybridní port, tedy hybrid port.

Na trunk portu jsou povoleny pouze tagované VLAN, paket či rámec, který nemá tag je zahozen. Tento port přenáší všechny pakety či rámce s VLAN tagem, které jsou povolné, konfigurace PVID bývá zde ignorována. Příkladné využití je pro propojení switchů a uplinku k routerům. [52]

Na access portu je pouze jedna netagovaná VLAN. Všechny pakety či rámce na tomto portu jsou zařazeny pouze do jedné VLAN sítě, nelze tedy využít více VLAN sítí. Hodnota PVID je nastavena na číslo netagované VLAN, typické použití je pro přípojení koncových stanic. [52]

Hybrid port je kombinací trunku s jednou netagovanou VLAN. Port přenáší tagované pakety či rámce, pokud paket či rámec nemá tag, je jím opatřen dle nastavení netagované VLAN, odrážející se od hodnoty PVID. Použití v praxi, může být například při přenosu IPTV a internetu. IPTV běží ve VLAN síti, internet pak v netagované VLAN síti. [52]

6 Link state routing protokoly

Jak už bylo zmíněné na začátcích této diplomové práce, tak TRILL protokol využívá rozšíření link state routing protokolu IS-IS.

Link state routing protokoly (LSP) pracují na principu, kdy si každý router zjistí, jaká má sousední zařízení stejného typu, v tomto případě jde o sousední routery a v pravidelných intervalech je testována jejich dostupnost za pomocí Hello paketu. Celá síť je následně zanesena vysíláním typu multicast ohledně toho, koho má konkrétní routovací zařízení za své sousedy. To znamená, že každý router má od všech ostatních routerů zprávu ohledně toho, jaká má sousední zařízení. Z toho plyne, že každý router má seznam všech cest v dané počítačové síti. Na tento seznam se aplikuje algoritmus nejkratší cesty, kterým se rozhoduje o směru, kam se má síťová jednotka odeslat. Jednotlivé položky směrovací (routovací) tabulky se počítají za pomocí algoritmu nejkratší cesty z dat získaných ze strany ostatních routerů. [40]

Link state routovací protokoly patří do skupiny IGP (Interior Gateway Protocol) protokolů, to znamená, že proces směrování se koná uvnitř autonomních systémů. Jinak tomu je v případě EGP (Exterior Gateway Protocol) protokolů, které vykonávají proces směrování mezi autonomními systémy. Druhým typem IGP protokolů je typ Distance-vector routing (DVR). Mezi Distance-vector routing protokoly patří RIP, RIP2, EIGRP a IGRP.

Mezi link state routing protokoly patří již dříve zmíněný IS-IS, od kterého TRILL protokol využívá prvky a tím druhým je protokol pro hledání nejkratší cesty, tedy OSPF.

6.1 IS-IS

IS-IS je link state routing protokol, který k určení routovacích tras používá SPF algoritmus. IS-IS protokol využívá hello pakety, které umožňují rychlou konvergenci počítačové sítě, při detekci změn v síti. IS-IS vyhodnocuje změny topologie a určuje, zda má být proveden úplný přepočet SPF algoritmus nebo výpočet částečné trasy PRC. [56]

6.2 OSPF

OSPF je základní představitelem link state routing protokolu. V paměti směrovače vytváří kompletní mapu celé sítě, které se říká topologická databáze, odborně nazvána jako Link State Database. Na základě informací z této databáze, potom pomocí SPF algoritmu provádí výpočty, které jsou potřebné k zjištění nejvíce ideální cesty do konkrétních počítačových sítí. [55]

Značnou výhodou OSPF protokolu, ve srovnání se staršími směrovacími protokoly, například s protokolem RIP, je jeho schopnost fungovat ve velkých sítích. Toho bylo dosaženo zavedením dvou úrovní hierarchie. Síť je rozdělená na takzvané oblasti, kterým se zde odborně říká area. Výpočet SPF algoritmu se spouští pro každou oblast samostatnou metodou. Z jedné oblasti do druhé oblasti se předávají pouze sumární informace. Změna topologie sítě v jedné oblasti nevyvolá přepočet SPF algoritmu v ostatních oblastech. [55]

7 Využití TRILL protokolu v praxi

TRILL protokol má v praxi využití převážně v datových centrech a v podnikových sítích. Právě proto, v praktické části této diplomové práce je provedena casy study pro nasazení TRILL protokolu do prostředí podnikové sítě typu LAN, která je simulována v programu, k tomu určenému.

7.1 Datová centra

Datové centrum (data center) je fyzické uspořádání serverů, ve kterých organizace v mnoha případech uchovávají jejich citlivá data či aplikace, například pro případ ztráty. Návrh datového centra je založen na počítačové síti, za pomocí výpočetních a úložných prostředků, které umožňují doručování sdílených dat a aplikací. Mezi klíčové síťové prvky k návrhu datového centra patří switche, routery, brány firewall, úložné systémy, servery a ovladače doručování aplikací. [41]

Moderní datová centra (data centers) se zcela liší realizací, než tomu bylo zvykem dříve. Infrastruktura sítě byla obvykle praktikována ve formě fyzických serverových zařízení. Moderní datová centra dnes fungují převážně ve formě virtuálních sítí, které podporují aplikace a vytížení napříč oblastmi fyzické infrastruktury a multicloudového prostředí. [41]

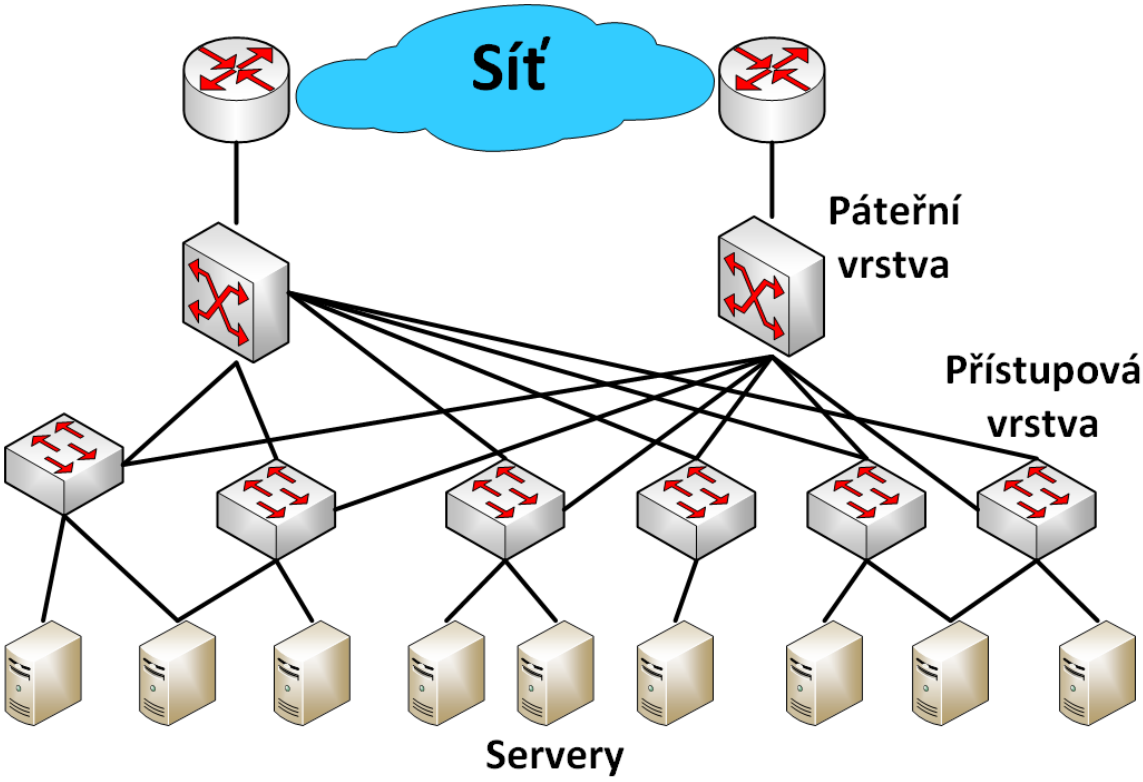
V současné době jsou data propojena mezi více datovými centry edge částí, veřejnými cloudovými prostředími a soukromými cloudovými prostředími. Datové centrum musí umět komunikovat mezi všemi těmito oblastmi, a to jak na straně lokálního prostoru, tak i na straně cloudového prostoru. Veřejné cloudové prostředí je ve své podstatě množina datových center. V případě, kdy jsou aplikace uzpůsobené v cloudovém prostředí (model SaaS), využívají tak prostředky datového centra ze strany poskytovatele cloudového prostředí. [41]

Data a aplikace pochopitelně v datových centrech musí být nějakým způsobem systematicky řízeny a ukládány, proto je zabezpečení datového centra nesmírně důležité při jeho návrhu. Z takového důvodu existují následující komponenty pro datová centra:

- **Infrastruktura pro úložiště (Storage infrastructure)** - Data jsou nezbytným prvkem pro existenci moderního datového centra. Systémy pro úložný prostor (storage systems) slouží pro jejich potřebné uchování.
- **Síťová infrastruktura (Network infrastructure)** – Tato infrastruktura slouží k propojování serverů, a to jak těch fyzických, tak i těch virtuálních, dále propojuje veškeré služby datových center, úložná místa a vnější propojení do míst koncových uživatelů.
- **Výpočetní prostředky** – Aplikace řídí datová centra. Tyto prostředky poskytují paměť, zpracování, místní úložiště a síťové připojení, které řídí aplikace.
  [41]

Datová centra se využívají například na podporu podnikových softwarů/systémů, mohou najít využití, například v oblasti Big data, umělé inteligence, ve virtuálních zařízeních, v podnikových systémech typu CRM či ERP, u produktivních softwarů nebo také i u souborového sdílení. [41]

Obrázek č. 8 znázorňuje typickou architekturu odkazující na moderní datové centrum, která oproti většině podnikových sítí, využívá pouze dvě vrstvy místo třech a to vrstvu přístupovou a vrstvu páteřní.

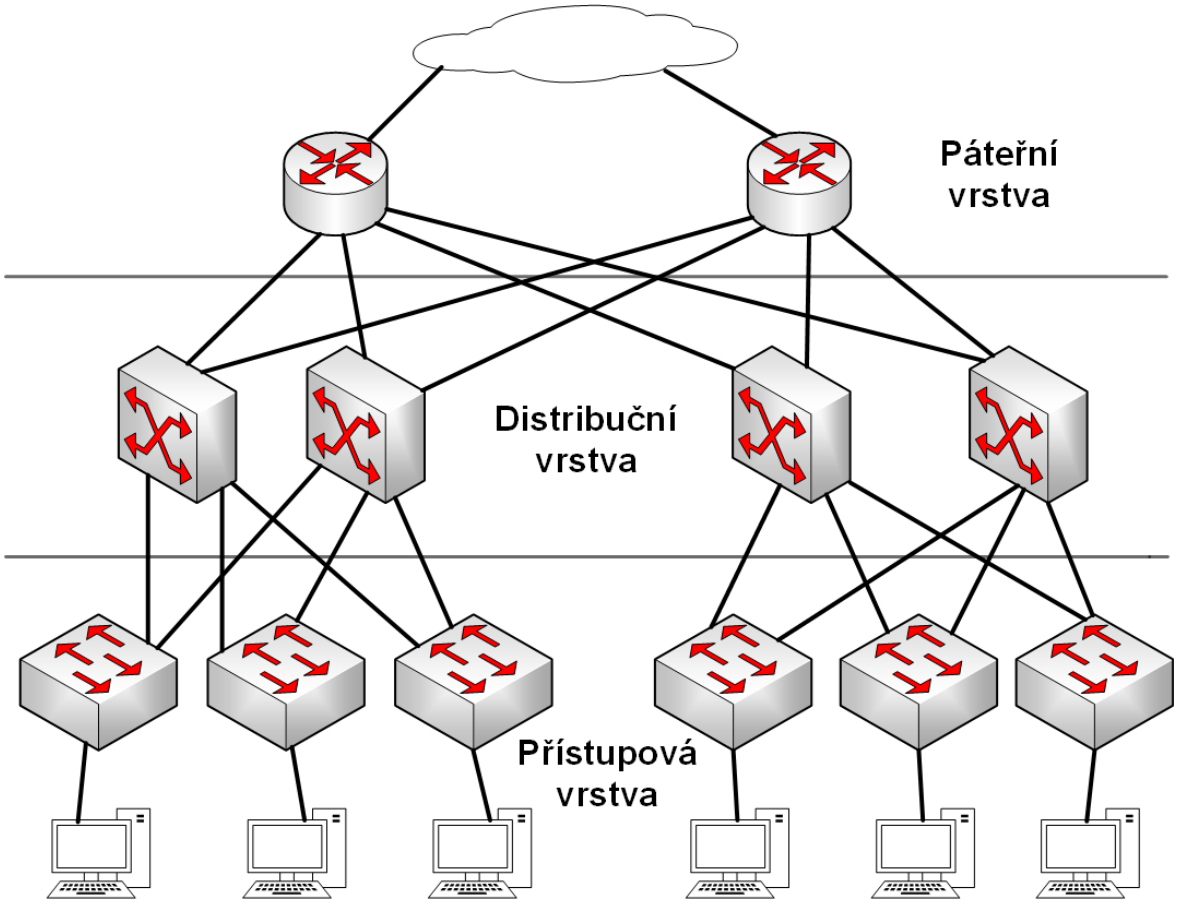


Obrázek 8 - Datové centrum

7.2 Podnikové sítě

Podnikové sítě bývají obvykle stavěny podle principu třívrstvé architektury, to znamená, že síťové prvky jsou rozděleny do přístupové vrstvy, do vrstvy distribuční a jako poslední do vrstvy páteřní. Podniková síť obsahuje libovolný počet malých podsítí, které jsou rozdělené pomocí zařízeních síťové vrstvy, tedy routerů a komunikace probíhá většinou ve směru od koncového zařízení až do oblasti internetu. [13]

Obrázek č. 9 znázorňuje typickou třívrstvou architekturu odkazující na podnikovou síť.



Obrázek 9 - Třívrstvá architektura podnikové sítě

Přepracováno od zdroje: Network Topology Architectures – IPCisco [54]

8 Nasazení protokolu TRILL

V praktické části této diplomové práce bylo cílem vytvořit simulaci pro fungování TRILL protokolu a jaké by mohlo být jeho nasazení v podnikové síti. Jelikož při zpracování této diplomové práce nebyla možnost využít fyzická RBridge zařízení pro nasazení TRILL protokolu do prostředí podnikové sítě. Důvodem je i pořizovací cena pro zařízení typu RBridge, a právě proto se ve softwarovém simulátoru vytvořila topologie, která by měla simulovat průměrnou podnikovou síť.

Simulovaná topologie pro průměrnou podnikovou síť se skládala jak ze zařízení typu RBridge, tak i z klasických switch zařízení typu Ethernet.

Pro síťovou simulaci byl zvolen simulátor eNSP (Enterprise Network Simulation Platform) od společnosti Huawei. Tento simulátor byl vybrán především z toho důvodu, že umožňuje pro simulaci využití prvků, které umí zprostředkovat funkce TRILL protokolu. Takové prvky v dané simulaci představují RBridge zařízení pro reálně nasazenou počítačovou síť.

8.1 eNSP Simulátor

Simulátor eNSP (Enterprise Network Simulation Platform) je softwarová platforma, která je bezplatně dostupná po registraci na stránkách společnosti Huawei. Jedná se o škálovatelnou platformu, která umí realizovat simulaci podnikových sítí. Simuluje hlavně routery, switche, brány firewall, WLAN sítě a další zařízení v podnikových sítích. Jeho rozhraní je zcela intuitivní a dokáže perfektně prezentovat zařízení v provozu v reálném čase. Simulátor eNSP podporuje škálování rozsáhlejší sítě a uživatelé tak mají možnost modelovat sítě při absenci pro dostupnost skutečného fyzického síťového vybavení. Současně je možné využít skutečnou síťovou kartu (NIC) k propojení se skutečným fyzickým síťovým zařízením, které dokáže přívětivěji zobrazit proces interakce s protokolem. To usnadňuje uživatelům učení a pochopení toho, jak fungují konkrétní síťové technologie. Simulátor eNSP pomáhá překonat veškerá omezení nedostatečných prostředků potřebných pro výuku počítačových sítí. Simulátor eNSP se snadno používá při tvorbě síťové simulace díky podpoře rozšiřitelného grafického uživatelského rozhraní (GUI). [57]

8.1.1 Instalace eNSP simulátoru

Instalace eNSP simulátoru není úplně jednoduchá na pár prostých kliknutí, jak by se na první pohled mohlo zdát, jako tomu je u běžných aplikací. K zajištění nekonfliktního nastavení pro používání platformy je potřeba před instalací splnit určité požadavky. K instalaci eNSP simulátoru bude také potřeba instalace dalších tří programů. Těmi jsou VirtualBox, WinPcap a Wireshark.

Každý z těchto tří programů ovládá své vlastní funkce pro spolupráci eNSP simulátoru. Virtualizační platforma VirtualBox od firmy Oracle poskytuje virtualizaci pro síťová zařízení, aby mohla být simulována dle obrazu skutečných síťových zařízení, na základě případného síťového scénáře. Programy pro síťovou analýzu Wireshark a WinPcap umožňují zachytávání paketů a rámců pro případnou analýzu pro odstraňování problémů. [49]

Při instalaci eNSP simulátoru byla instalovaná u VirtualBoxu verze 5.2.44, protože novější verze 6 a vyšší mají u simulátoru eNSP problémy s kompatibilitou. V tomto případě

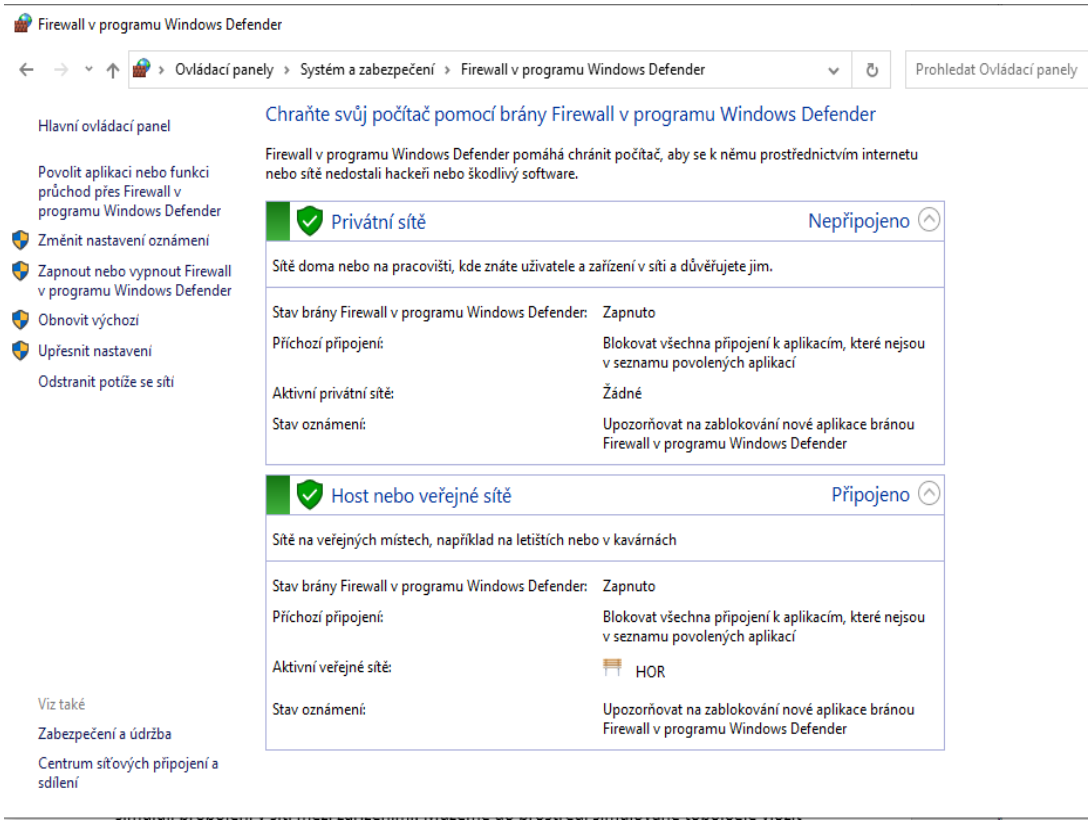
je zvolení pozdější verze VirtualBoxu velice důležitým krokem. Z podobného důvodu byla instalována verze 4.1.3 u programu WinPcap. [49]

Pro instalaci dodatečných tří programů je zcela důležitá posloupnost, jak budou po sobě instalovány. Je to z toho důvodu, že některé softwarové komponenty jsou závislé a některé zase naopak závislé nejsou. Programy, které závislé nejsou, musí být nezbytně nainstalovány dříve než programy, které závislé jsou. U eNSP simulátoru závisí na tom, aby dodatečné tři programy byly nainstalovány správně, proto samotný simulátor bude kompletně nainstalován až po instalaci zmíněných tří programů. Veškeré instalace by se měly provádět v režimu administrátora. [49]

Prvním programem, kterým se zahájí instalace je WinPcap. Pokračuje se instalací Wiresharku a do třetice dochází na instalaci virtualizační platformy VirtualBox.

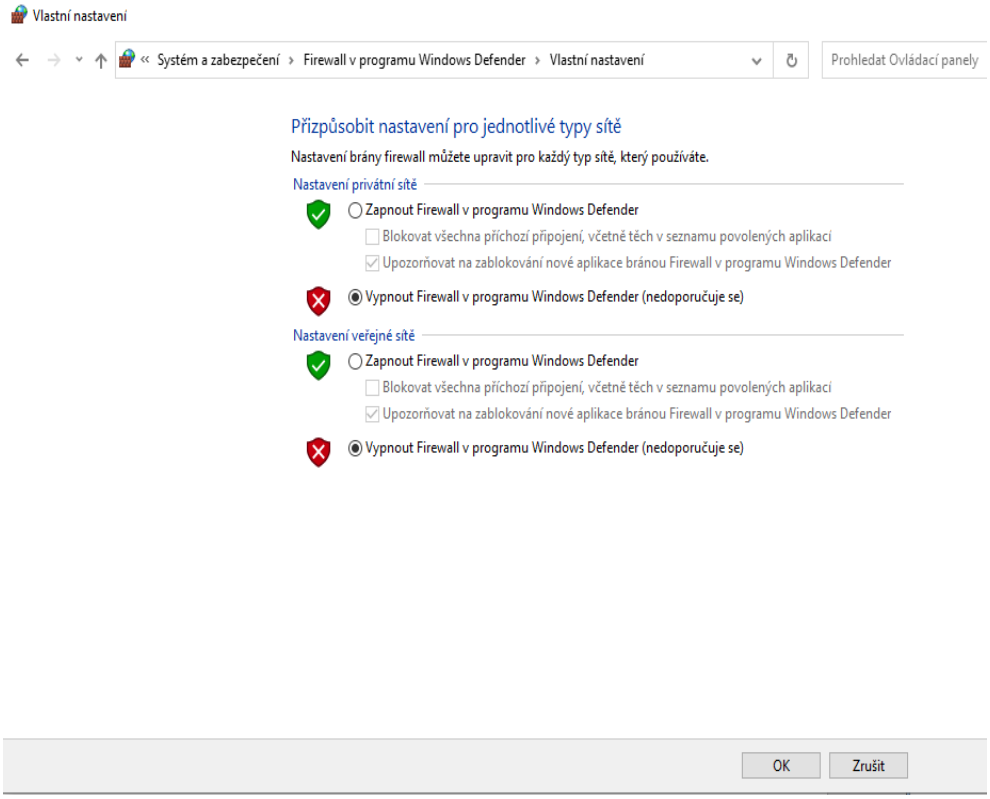
Poté, co se dokončí instalace všech těchto tří potřebných programů, se může konečně zahájit instalace samotného eNSP simulátoru. Ovšem, než dojde k samotnému zahájení, měla by se u operačního systému Windows deaktivovat brána firewall, případně pokud je brána firewall aktivována neimplicitně v nějakém programu třetích stran, měla by být před instalací eNSP simulátoru deaktivována i tam.

Obrázek č. 10 zobrazuje, jaké okno se ukazuje, když je brána firewall aktivována na straně programu Windows Defender. V takovém případě by se mohly při instalaci eNSP simulátoru vyskytnout problémy a mělo by to i negativní vliv na některé funkce daného simulačního prostředí, například při importu dodatečných zařízení. Proto je potřeba pro bránu firewall zde nastavit výjimku a před instalací eNSP simulátoru jí u programu Windows Defender deaktivovat.



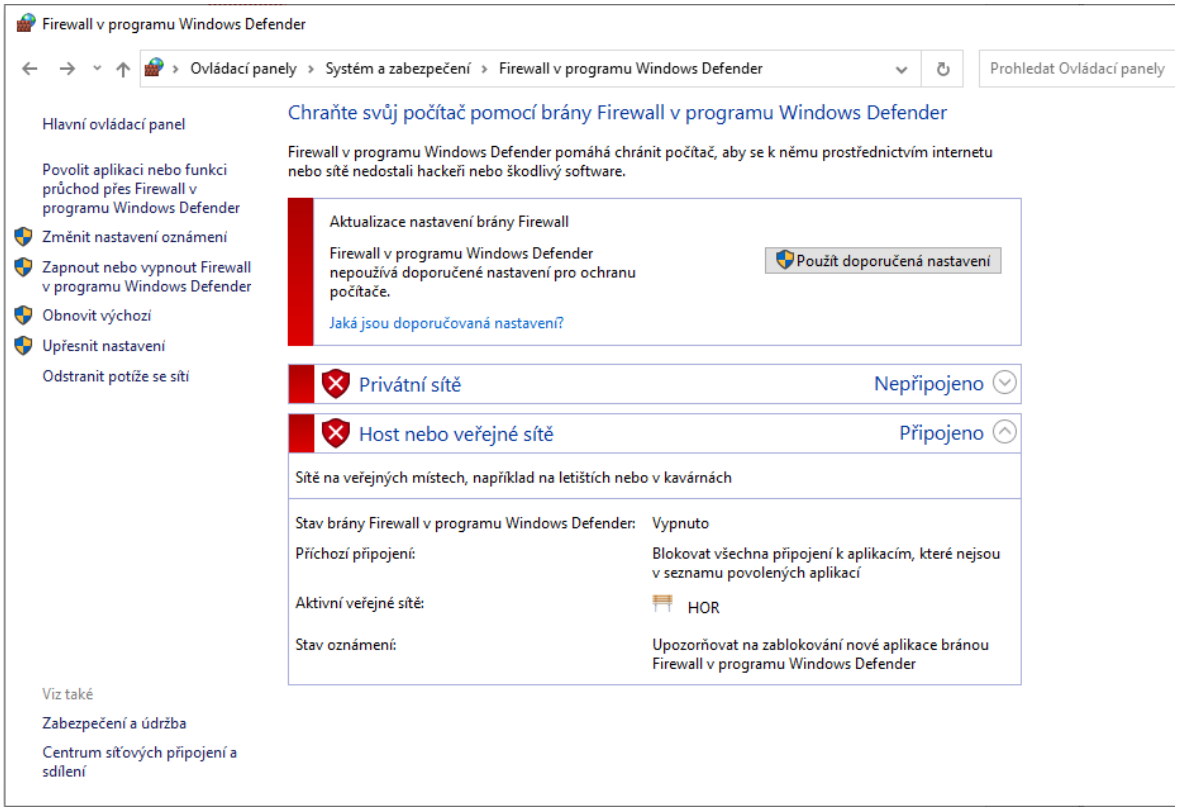
Obrázek 10 - Aktivována brána firewall ve Windows

Obrázek č. 11 zobrazuje, kde je potřeba vypnout bránu firewall, tak aby nezpůsobovala problémy při instalaci a následného správného chodu prostředí pro eNSP simulátor. Brána firewall se pro jistotu deaktivuje, jak v privátní síti, tak i v síti veřejné.



Obrázek 11 - Deaktivace brány firewall

Obrázek č. 12 zobrazuje, jaké okno se znázorňuje, když je brána firewall deaktivována na straně programu Windows Defender a to, jak u privátní sítě, tak i u sítě veřejné. V takovém případě by už mělo být vše v pořádku a instalace eNSP simulátoru se může bez problému zahájit.



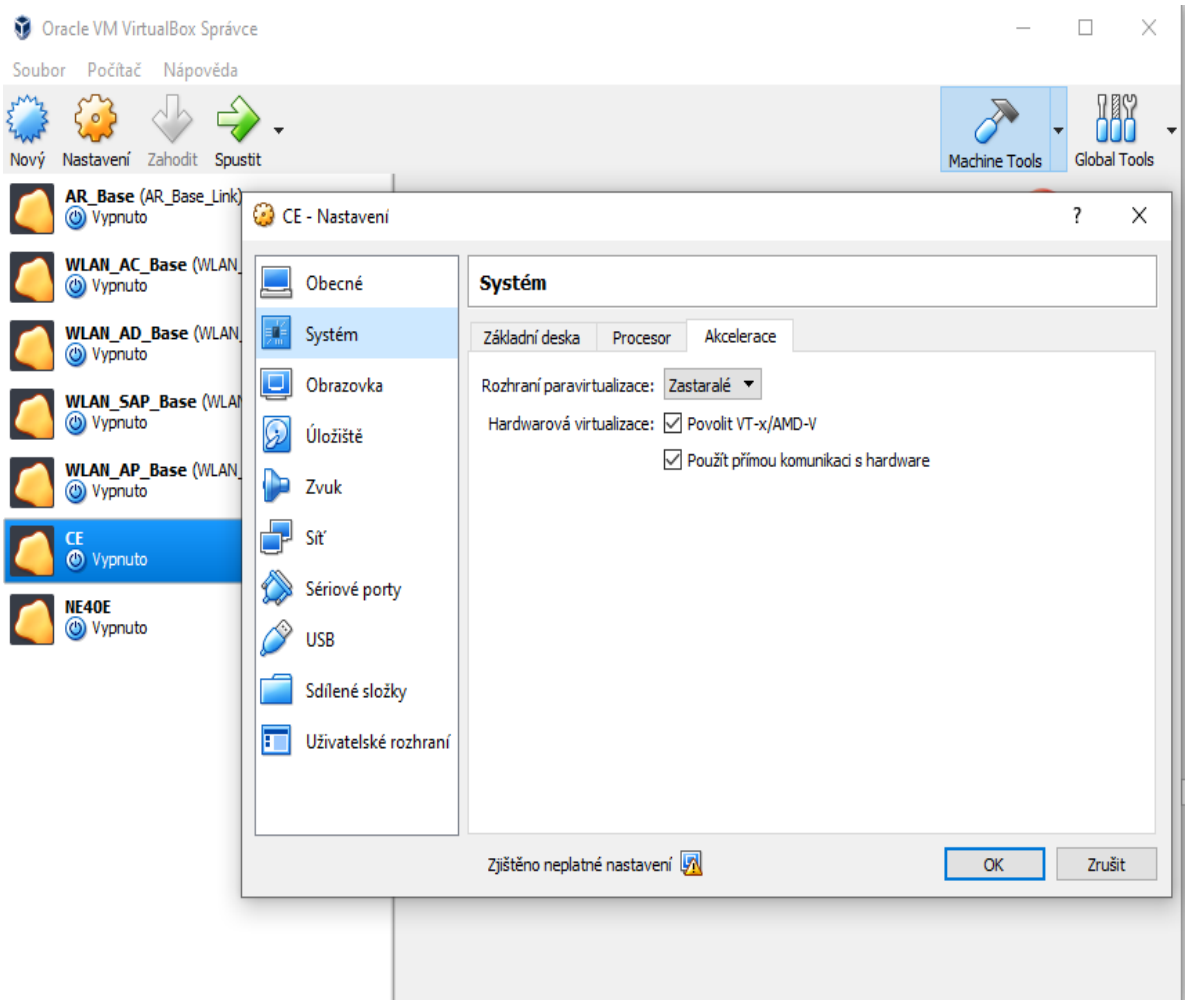
Obrázek 12 - Deaktivovaná brána firewall ve Windows

8.1.2 Podpora virtualizace

K pokrokovému zlepšení při využívání prostředků a výkonu virtuálních zařízení existují hardwarová rozšíření, od obou dlouhodobě na trhu hlavních výrobců procesorů (CPU), kterými jsou Intel a AMD. Jsou to technologie Intel VT-x a AMD-V. Virtualizace, která je prováděna pouze za pomocí softwarového vybavení může mít nepřijatelně pomalý proces, a právě proto využití takových technologií procesoru (CPU) mohou užitečně pomoci při vykonávání určité činnosti. Výrazným způsobem se může zlepšit výkon aplikací ve virtuálním prostředí. [49]

K účelnému využití této doplňkové funkce implementované na základní desce (motherboard) při simulaci podnikové sítě u eNSP simulátoru, je potřeba ji aktivovat v nastavení BIOSu či UEFI.

Následující obrázek č. 13 jasně zobrazuje, že hardwarová virtualizace je pro virtualizační platformu VirtualBox a pro síťový simulátor eNSP k dispozici. Při vykonávání praktické části této diplomové práce byla konkrétně využita technologie AMD-V.



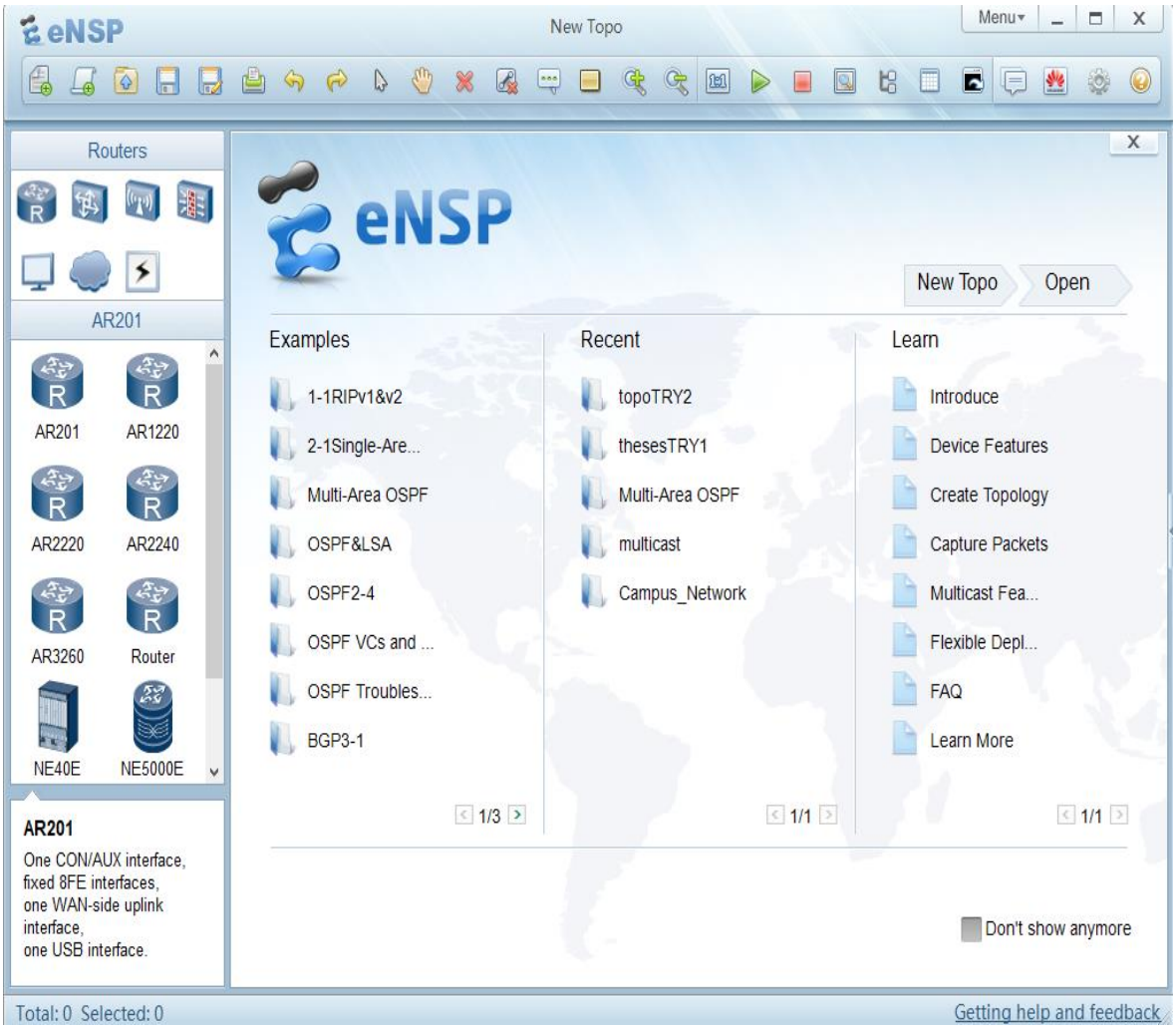
Obrázek 13 - Podpora virtualizace

8.1.3 Spuštění eNSP simulátoru

Po otevření spustitelného souboru pro eNSP simulátor se nám objeví následující okno zobrazené na obrázku č. 14.

V horní liště, pod logem eNSP simulátoru a názvem případného otevřeného projektu, vidíme panel s ovládacími prvky. Pomocí těchto ovládacích prvků můžeme vytvořit nový projekt se simulovanou topologií nebo také otevřít už dříve vytvořený projekt. Následně zde máme takové ty klasické ovládací prvky pro uložení projektu, pro tisk, tlačítko vpřed a zpět, výběr, ukazatele, vymazání konkrétní části, případně vymazání všech čár, které zde simulují propojení v síti mezi zařízeními. Můžeme do prostředí simulované topologie vložit i textová pole pro popisky. Máme zde k dispozici i kreslící paletu, která nám umožňuje do prostředí vkládat barevné čáry či základní geometrické tvary, kromě barvy je možné si zvolit šířku a styl ohraničení. Nechybí zde ani přibližování a oddalování, případně i reset zoomování. Klíčovým ovládacím prvkem je zde ovládací prvek „Start device“, který umožňuje uvést do chodu konkrétní síťové zařízení, případně i skupinu síťových zařízení, když se označí hromadně. Vedle toho můžeme i chod takto spuštěných síťových zařízení pochopitelně i zastavit, a to pomocí ovládacího prvku „Stop device“. Dále můžeme zachytávat data pomocí ovládacího prvku „Capture Data“ pro případnou nastávající síťovou analýzu s asistencí programu Wireshark. Posledními ovládacími prvky jsou možnosti pro zobrazení všech rozhraní (interface) či případně jeho skrytí, zobrazení

mřížky a v poslední řadě otevření všech příkazových řádků CLI pro všechny aktivní síťové prvky v dané simulované topologii. Zleva vidíme sloupec, který nám ukazuje síťové prvky, které se mohou vložit do prostředí simulované síťové topologie. Vložení síťového prvku se do prostředí pro simulovanou síťovou topologii provede pouhým jednoduchým přetažením. V části, kde při spuštění či zahájení projektu bývá prostředí pro simulovanou síťovou topologii, vidíme část „Examples“, kde je k dispozici řada ukázkových hotových síťových topologií. Hned vedle je část „Recent“, která zobrazuje posledně spuštěné projekty. A poslední je část „Learn“, která obsahuje kvalitní dokumentaci, například k tomu, jak používat program eNSP, jak ovládat jeho funkce atd.



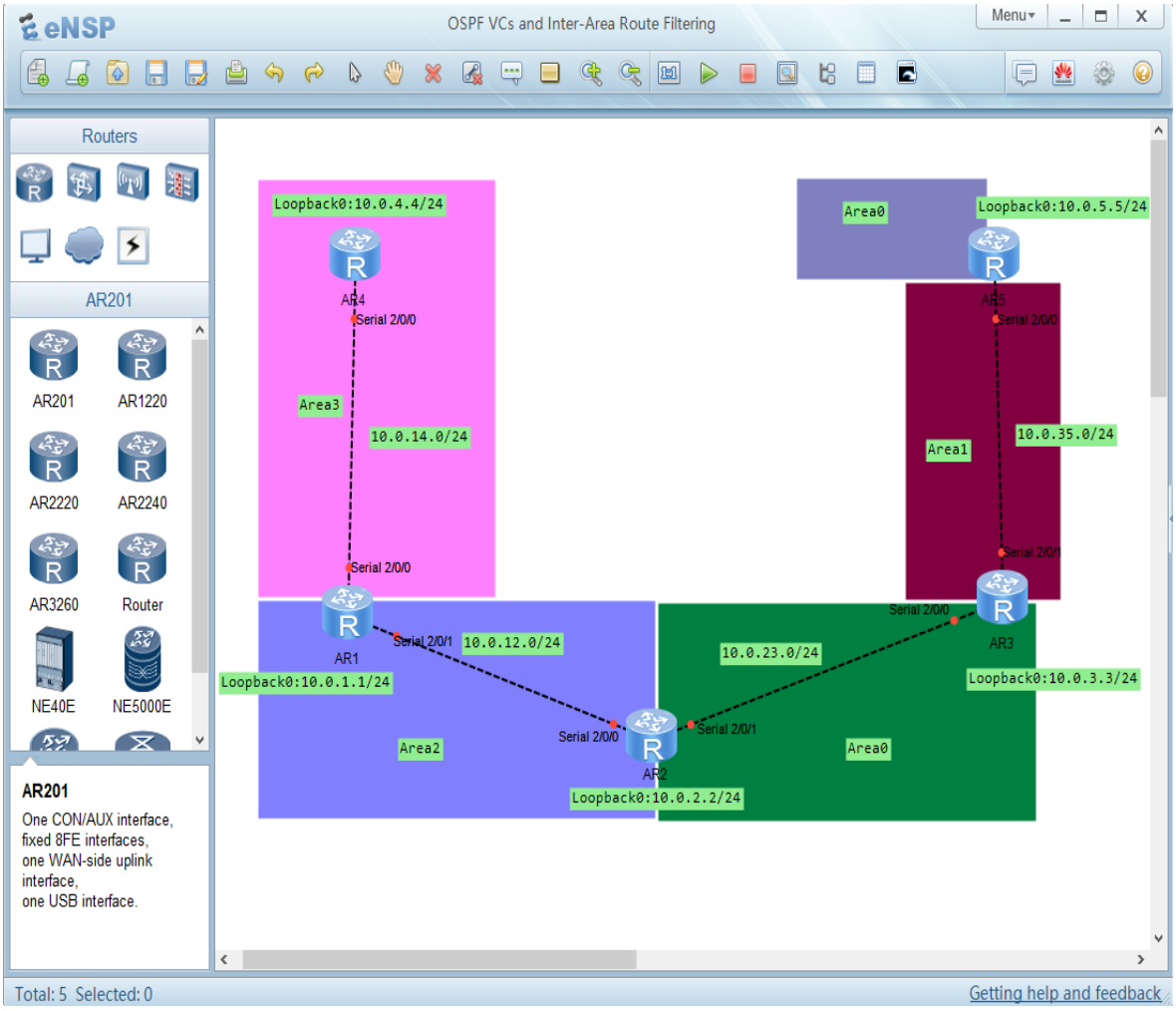
Obrázek 14 - Úvodní okno eNSP simulátoru

8.1.4 Ukázková hotová topologie

Jak už bylo zmíněno výše, tak eNSP simulátor, obsahuje řadu ukázkových hotových síťových topologií, které můžou sloužit například pro inspiraci při tvorbě simulace.

Obrázek č. 15 zobrazuje právě jednu vybranou hotovou síťovou topologii, která je založena na principu link state routovacího protokolu OSPF. Ve vybrané simulované síťové topologii je vidět pět rozmístěných routerů, označených zkratkou AR, které jsou mezi sebou propojené rozhraním typu Serial. Nepřehlédnutelné jsou zde vyskytující se barevné obdélníky, které v simulované síťové topologii jsou z větší části grafickou

ozdobou. Takové pouhé grafické vyladění může například zdůrazňovat konkrétní úseky v topologii dané simulované sítě, jako tomu je i například zde, v konkrétní ukázkové topologii. V poslední řadě zde vidíme různé popisky, které se týkají názvů oblastí, IP adres síťových zařízení a spojů s jejich prefixem a také názvů jednotlivých rozhraní (interface).



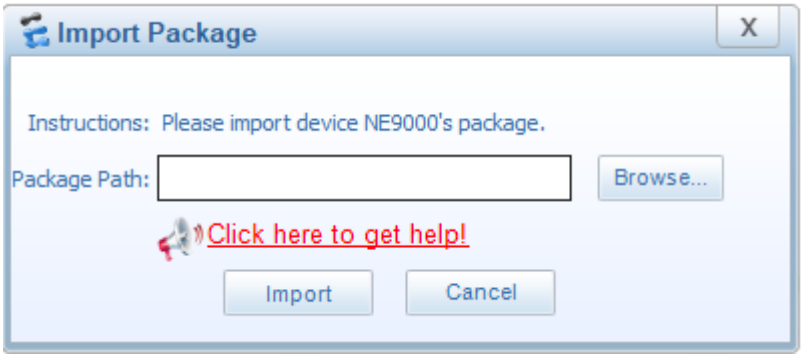
Obrázek 15 - Ukázka hotové simulované topologie

8.2 Simulace topologie pro podnikovou síť

Pro simulaci síťové topologie, která má znázorňovat podnikovou síť a case study, pro nasazení TRILL protokolu do ní, bude využita třívrstvá architektura, protože tomu tak bývá v praxi zvykem u podnikových sítí většího rozsahu. Zmíněná třívrstvá architektura se skládá ze směru dolní části z přístupové vrstvy, o řád výše jde o vrstvu agregační a poslední vrstvou je páteřní vrstva.

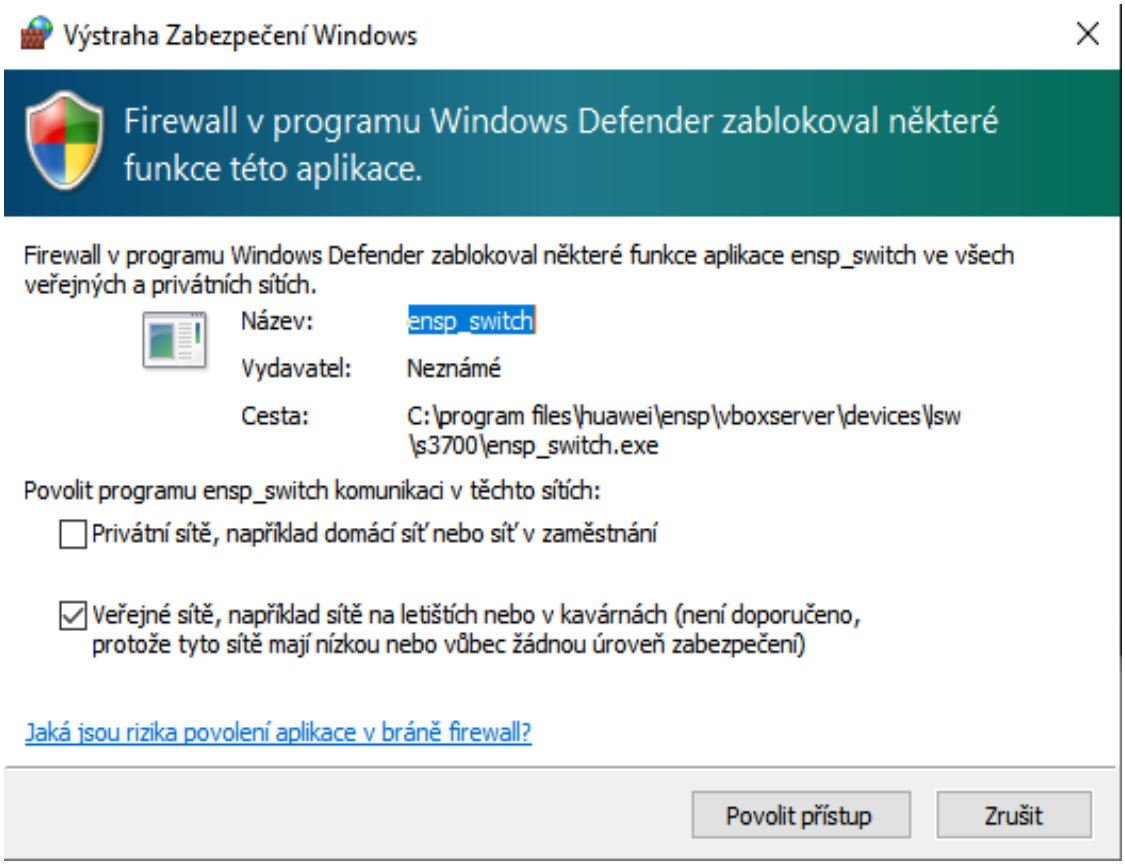
Jak už bylo zmíněno v teoretické části této diplomové práce, tak switch zařízení, která fungují na principu TRILL protokolu jsou odborně nazývány jako RBridge (Routing Bridge) nebo se pro ně i někdy používá název TRILL switch. Do simulace síťové topolegie pro case study se použily switch zařízení CE6800 (CloudEngine 6800), která umí fungovat na principu protokolu TRILL. Jelikož se jedná o typ zařízení, které není základní součástí nainstalovanou společně s eNSP simulátorem, tak při prvním spuštění zařízení typu CE6800 vyskočí následující okno zobrazené na obrázku č. 16, v prostředí eNSP simulátoru, které bude vyžadovat import balíčku pro konkrétní typ zařízení. Do importu se

vloží obraz disku (IMG) se souborovou příponou „.img“, který odkazuje na konkrétní síťový prvek a poté se s daným naimportovaným prvkem může bez problému pracovat.



Obrázek 16 - Import typu zařízení

V průběhu používání některých prvků či funkcí eNSP simulátor může dojít k tomu, že s nimi bude mít brána firewall problém a bude chtít blokovat některé funkce. To se pozná tak, že se objeví dialogové okno, které bude žádat o povolení přístupu. V takovém případě stačí pouze povolit přístup a pro daný prvek či funkci už by se taková situace v programu neměla vyskytnout.

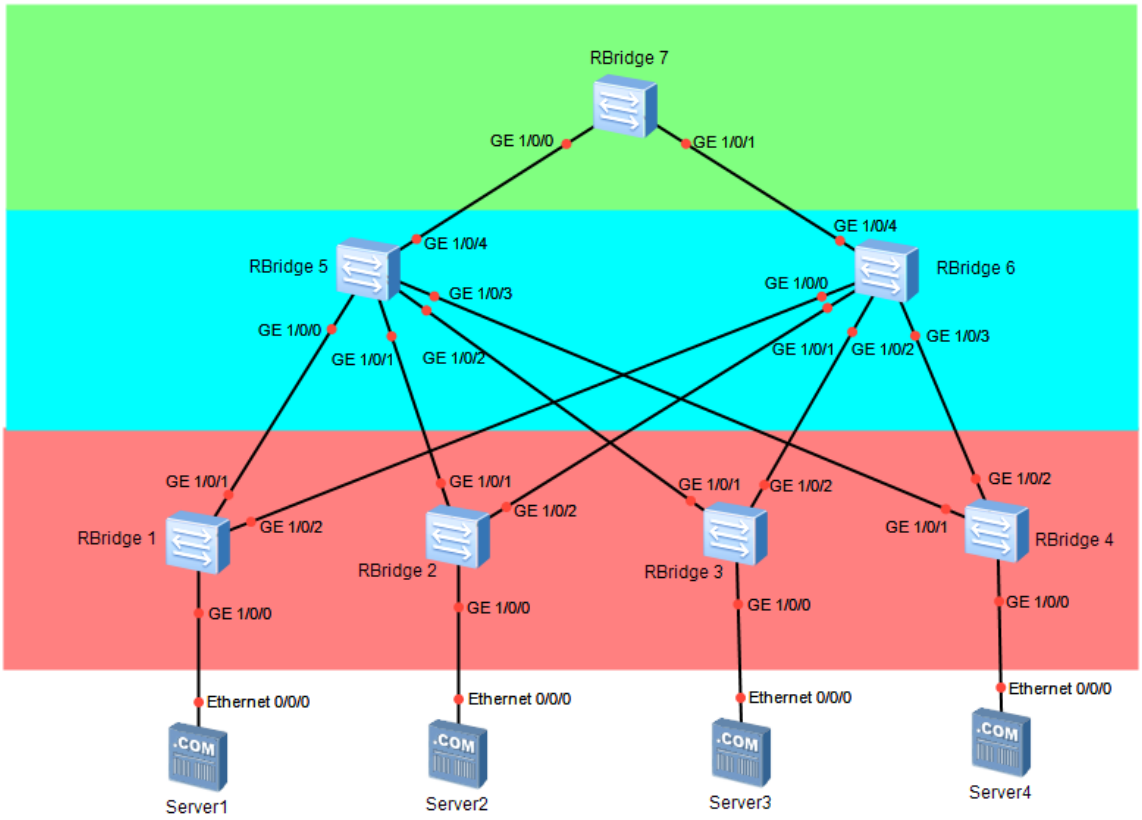


Obrázek 17 - Potřeba výjimky u brány firewall

8.2.1 Simulace topologie pro podnikovou síť při nasazení TRILL protokolu

První varianta simulující topologii pro podnikovou síť byla stavěna na situaci, která by předpokládala, že prostředí podniku bude mít k dispozici finanční možnosti na vybudování RBridge zařízení ve všech místech třívrstvé architektury, a proto se v topologii nevyskytuje ani jeden klasický switch typu Ethernet, jak je názorně vidět na obrázku číslo 18.

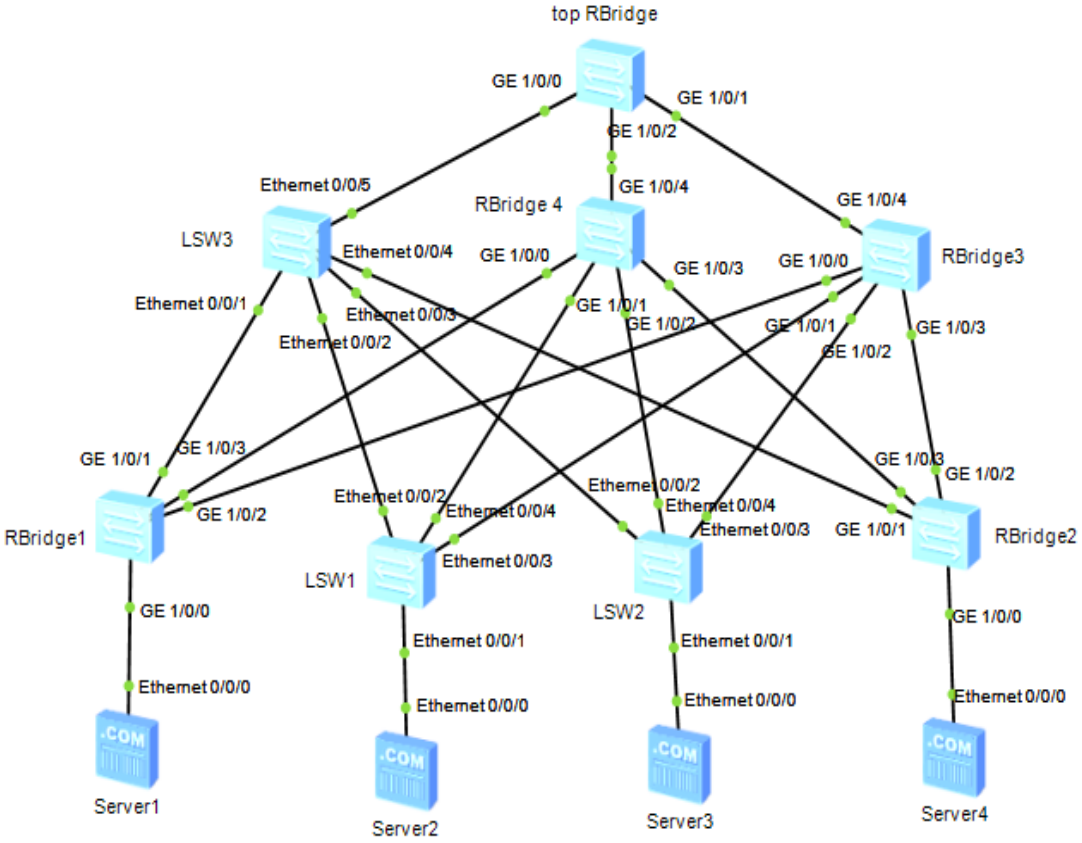
Červený obdélník znázorňuje přístupovou vrstvu (access layer) pro třívrstvou architekturu, světle modrý obdélník znázorňuje vrstvu agregační (distribution layer) a nejvyšší vrstva, tedy vrstva páteřní (core layer) je znázorněna v zeleném obdélníku.



Obrázek 18 - Topologie simulované podnikové sítě s nasazením RBridgů na všech místech

8.2.2 Simulace topologie pro podnikovou síť při nasazení TRILL protokolu s kombinací STP protokolu

Druhá varianta simulující topologii pro podnikovou síť byla stavěna na situaci, která by počítala s tím, že prostředí podniku nebude mít finanční či kterékoliv jiné možnosti na vybudování RBridge zařízení, ve všech místech třívrstvé architektury, a proto je následující topologie kombinací, jak RBridge zařízení, tak i klasických switchů typu Ethernet, jak je názorně vidět na obrázku číslo 19.



Obrázek 19 - Topologie simulované podnikové sítě pří nasazení TRILL protokolu s kombinací STP protokolu

8.2.3 Porovnání obou variant simulací topologie

Obrázek č. 20 znázorňuje routovací tabulku z první varianty simulace, kde v architektuře podnikové sítě byly implementovány pouze RBridge zařízení.

```
[~RBridge1]display trill route

TRILL Unicast Routing Table
------------------------------------------------------------------------------

Flags: D-Download To Fib

Total Route(s): 6

Nickname      Cost  Flag  OutInterface     OuterVlan  NextHop              Hop
------------------------------------------------------------------------------
     200    400000  D     GE1/0/1                 10  500/707b-e89b-7491     2
     300    400000  D     GE1/0/1                 10  500/707b-e89b-7491     2
     400    400000  D     GE1/0/1                 10  500/707b-e89b-7491     2
     500    200000  D     GE1/0/1                 10  500/707b-e89b-7491     1
     600    200000  D     GE1/0/2                 10  600/707b-e89a-4f77     1
     700    400000  D     GE1/0/1                 10  500/707b-e89b-7491     2
[~RBridge1]
```

Obrázek 20 - Zobrazení trasování při všech RBridgů v jedné architektuře

Obrázek č. 21 znázorňuje routovací tabulku z druhé varianty simulace, kde v architektuře podnikové sítě byly implementovány kombinace RBridge zařízení a klasických switchů typu Ethernet.

```
[~RBridge1]display trill route

TRILL Unicast Routing Table
------------------------------------------------------------------------------

Flags: D-Download To Fib

Total Route(s): 4

Nickname      Cost  Flag  OutInterface     OuterVlan  NextHop              Hop
------------------------------------------------------------------------------
     200    400000  D     GE1/0/2                 10  300/707b-e8b8-5bbb     2
                          GE1/0/3                 10  400/707b-e89b-6f02     2
     300    200000  D     GE1/0/2                 10  300/707b-e8b8-5bbb     1
     400    200000  D     GE1/0/3                 10  400/707b-e89b-6f02     1
     500    400000  D     GE1/0/2                 10  300/707b-e8b8-5bbb     2
                          GE1/0/3                 10  400/707b-e89b-6f02     2
```

Obrázek 21 - Zobrazení trasování při kombinaci RBridgů a klasických Ethernet switchů v jedné architektuře

Z obou obrázků č. 20 a č. 21 je jasně vidět, že při vícecestném směrování je první varianta méně vytížená než varianta druhá. Na obrázku č. 21 je vidět zpoždění při skoku ze zařízení s nickname hodnotou 200, k zařízení s nickname hodnotou 300. Takové situace se u první varianty na obrázku č. 20 nevyskytuje.

Závěr

Hlavním cílem této diplomové práce bylo podrobně zpracovat principy protokolu TRILL (Transparent Interconnection of Lots of Link) a následně provést jeho simulaci pro potencionální možnosti při implementaci do podnikové sítě. Diplomová práce se pro případ podnikových sítí zaměřovala konkrétně na sítě lokální, tedy LAN (Local Area Network).

V teoretické části diplomové práce byl podrobně představen protokol TRILL, včetně jeho principů a funkcí. Následně byl v této diplomové práci podrobně představen i protokol STP (Spanning Tree Protocol), který má TRILL protokol v počítačových sítích nahrazovat, což bylo dokonce i jeho původním účelem při jeho uvedení. U STP protokolu byly představeny i jeho modifikované verze, kterými jsou RSTP, MSTP a PVST, případně PVST+.

Jelikož TRILL protokol nebyl jedinou technologií, která měla za původní účel nahradit STP protokol, byly představeny i jemu podobná řešení, kterými konkrétně jsou FabricPath od společnosti Cisco a technologie SPB (Shortest Path Bridging). S SPB technologií došlo k důkladnému porovnání s velkým počtem srovnávacích kritérií.

Jak už bylo zmíněno výše, že simulované topologie se zaměřovaly výhradně na počítačové sítě typu LAN, jak už název diplomové práce napovídá, tak z toho důvodu byly v teoretické části této diplomové práce představeny i obecné základy počítačových sítí, včetně referenčního modelu ISO/OSI. Kromě počítačové sítě typu LAN byly stručně představeny i ostatní členění počítačových sítí dle rozsahu, kterými jsou PAN, MAN, CAN, GAN a WAN.

V praktické části diplomové práce byly představeny varianty simulací pro nasazení TRILL protokolu v prostředí podnikové sítě typu LAN. Simulace podnikové sítě byla stavěna na modelu třívrstvé architektury. Simulované prostředí podnikové sítě bylo vytvořené v síťovém simulátoru eNSP (Enterprise Network Simulator platform) od společnosti Huawei.

Na základě case study založené na vytvořených variantách simulovaných topologií představujících podnikové sítě bylo zjištěno, jak nasazení TRILL protokolu umožňuje v dané počítačové síti vícecestné (multi-path) směrování a jak dochází v počítačové síti za jeho pomoci k menšímu vytížení, než je tomu v případě pouhého nasazení klasických switchů typu Ethernet, které zvládnou maximálně STP protokol.

Seznam obrázků

Seznam tabulek

Seznam zkratek

TRILL	Transparent Interconnection of lots links
IETF	Internet Engineering Task Force
PC	Personal Computer
OS	Operating System
CPU	Central Processing Unit
GUI	Graphical User Interface
LAN	Local Area Network
VLAN	Virtual Local Area Network
MAN	Metropolitan Area Network
CAN	Campus Area Network
PAN	Personal Area Network
WAN	Wide Area Netwok
GAN	Global Area Network
STP	Spanning Tree Protocol
RSTP	Rapid Spanning Tree Protocol
MSTP	Multiple Spanning Tree Protocol
PVST	Per VLAN Spanning Tree (někdy značené PVST+)
PVSTP	Per VLAN Spanning Tree Protocol
RFC	Request For Comments
RB	Root Bridge
RBridge	Routing Bridge
RBs	Routing Bridges (RBridges)
DB	Designated Bridge
DRB	Designated Routing Bridge (DRBridge)
VL RB	VLAN Labeled Routing Bridge (VL RBridge)
L1	Layer 1
L2	Layer 2
L3	Layer 3
L4	Layer 4

L5	Layer 5
L6	Layer 6
L7	Layer 7
ISO	International Organization for Standardization
OSI	Open Systems Interconnection
ISO/OSI	International Organization for Standardization/ Open Systems Interconnection
LSP	Link State PDU (Protocol Data Unit)
LSRP	Link State Routing Protocol
DVR	Distance-vector routing
IGP	Interior Gateway Protocol
EGP	Exterior Gateway Protocol
IS-IS	**I**ntermediate System to Intermediate System
OSPF	Open Shortest Path First
RIP	Routing Information Protocol
IGRP	Interior Gateway Routing Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
SPT	Shortest Path Tree
ECMP	Equal-cost multi-path routing
IP	Internet Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/ Internet Protocol
B	Byte
MAC	Media Access Control
SPB	Shortest Path Bridging
SPF	Shortest Path First
IEEE	Institute of Electrical and Electronics Engineers
CRC	Cyclic Redundancy Check
TCI	Tag Conrol Information
V	Version
TTL	Time To Life

CHBH	Critical Hop by Hop
CItE	Critical Ingress to Egress bit
HDD	Hard Disc Drive
SSD	Solid State Drive
PDU	Protocol Data Unit
TLV	Type length value
NIC	Network Interface Controller
FGL	Fine-Grained Labeling
PRI	Priority field
DEI	Drop Eligibility Indicator
VL	VLAN (Virtual Local Area Network) Labeled
BPDU	Bridge Protocol Data Units
ID	Identifikace (Indetification)
SPBV	Shortest Path Bridging VLAN (Virtual Local Area Network)
SPBM	Shortest Path Bridging Mac-in-Mac
SPBVID	Shortest Path VLAN ID (Virtual Local Area Network Identification)
BVID	Backbone VLAN ID
BMAC	Backbone MAC (Media Access Control)
ESADI	End System Address Distribution Information
RPFC	Reverse Path Forwarding Check
BCB	Backbone Core Bridge
BEB	Backbone Edge Bridge
OAM	Operations, Administration and Maintenance (Management)
MPLS	Multiprotocol Label Switching
VPN	Virtual Private Network
RSVP	Resource reservation protocol
LDP	Label Distribution Protocol
BGP	Border Gateway Protocol
MP-BGP	Multiprotocol BGP (Border Gateway Protocol)
BID	Bridge ID

SaaS	Software as a Service
eNSP	Enterprise Network Simulation Platform
CLI	Command Line Interface
AMD	Advanced Micro Devices
AMD-V	Advanced Micro Devices – Virtualization (AMD – Virtualization)
VT-x	Virtual Technology – x
BIOS	Basic Input-Output System
UEFI	Unified Extensible Firmware Interface
AR	Area Router
GE	Gigabit Ethernet
CE	Cloud Engine
ISL	Inter-Switch Link
ERP	Enterprise Resource Planning
CRM	Customer Relationship Management
PRC	Partial Route Computation
DHCP	Dynamic Host Configuration Protocol
FTP	File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
POP3	Post Office Protocol

Seznam použité literatury

[1] **HOODA**, Sanjay K., Shyam KAPADIA a Padmanabhan KRISHNAN. Using TRILL, FabricPath and VXLAN: [designing massively scalable data centers with overlays]. Indianapolis, IN: Cisco Press, [2014]. ISBN 9781587143939.

[2] **LIU**, Yang. Data center networks. New York: Springer, 2013. ISBN 9783319019482.

[3] **Ing. Miroslav Matuška, Ph.D:** TRILL 2. část – Základní principy. Lupa.cz, říjen 2010. Dostupné z: https://www.lupa.cz/clanky/trill-2-cast-zakladni-principy/

[4] **Ing. Miroslav Matuška, Ph.D:** TRILL: Konečně náhrada za Spanning Tree?. Lupa.cz, říjen 2010. Dostupné z: https://www.lupa.cz/clanky/trill-konecne-nahrada-za-spanning-tree/

[5] **Autor neznámý:** Cloud Fabric Data Center Basic Network Solution Design – TRILL based Implementation. Huawei, 2014. Dostupné z: https://actfornet.com/HUAWEI_SWITCH_DOCS/All_Docs/HUAWEI%20Cloud%20Fabric%20Data%20Center%20Solution%20TRILL%20Design%20Guide.pdf

[6] **Ahmed AMAMAOU**, Kamel HADDADOU a Guy PUJOLLE. A TRILL-based multi-tenant data center network. Computer Networks: ScienceDirect, srpen 2014. Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S1389128614000851

[7] **Joe Touch** a **Radia Perlman**: RFC 5556: Transparent Interconnection of Lots of Links (TRILL): Problem and Applicability Statement. Network Working Group, květen 2009. Dostupné z: https://datatracker.ietf.org/doc/html/rfc5556#section-2

[8] **Andrey Baginyan**, Vladimir Korenkov, Andrey Dolbilov, Ivan Kashunin. Equal-cost multi-pathing in high power systems with TRILL. JINR, Laboratory of Information Technologies, září 2019. Dostupné z: https://www.epj-conferences.org/articles/epjconf/abs/2019/19/epjconf_chep2018_08013/epjconf_chep2018_08013.html

[9] **Autor neznámý:** TRILL Technology White Paper. H3C, srpen 2018. Dostupné z: http://www.h3c.com/en/d_201808/1102744_294549_0.htm

[10] **Mark Lippitt, Erik Smith** a **David Hughes**: Fibre Channel over Ethernet (FCoE) Data Center Bridging (DCB) Concepts and Protocols. EMC Corporation, 2015. Dostupné z: https://www.delltechnologies.com/asset/zh-tw/products/storage/technical-support/h6290-fibre-channel-over-ethernet-techbook.pdf

[11] **Donald E. Eastlake:** The IETF TRILL Protocol Transparent Interconnection of Lots of Links. Huawei, únor 2013. Dostupné z: https://conference.apnic.net/35/pdf/trillapricot8_1361288177.pdf

[12] **Adam Surák:** Transparent Interconnection of Lots of Links (TRILL) jako náhrada Spanning Tree. VŠB Technická univerzita Ostrava, květen 2012. Dostupné z: http://wh.cs.vsb.cz/sps/images/8/88/TRILL.pdf

[13] **Ing. Tomáš Kmoníček:** Analýza využití protokolu TRILL v podnikové síti. Univerzita Pardubice Fakulta elektrotechniky a informatiky, květen 2015. Dostupné z: https://dk.upce.cz/bitstream/handle/10195/60413/KmonicekT_AnalyzaVyuziti_JH_2015.pdf?sequence=1&isAllowed=y

[14] **Ing. Miroslav Matuška, Ph.D:** TRILL 4. část – Stav vývoje a alternativní řešení. Lupa.cz, říjen 2010. Dostupné z: https://www.lupa.cz/clanky/trill-4-cast-stav-vyvoje-a-alternativni-reseni/

[15] **Donald Eastlake, Anoop Ghanwani, Vishwas Manral, Yizhou Li** a **Caitlin Bestler:** RFC 7179: Transparent Interconnection of Lots of Links (TRILL): Header Extension. Internet Engineering Task Force (IETF), květen 2014. Dostupné z: https://datatracker.ietf.org/doc/html/rfc7179

[16] **Autor neznámý:** Cyclic Redundancy Check (CRC). Techopedia, září 2020. Dostupné z: https://www.techopedia.com/definition/1793/cyclic-redundancy-check-crc#what-does-cyclic-redundancy-check-crc-mean

[17] **Vladimír Veselý, Marcel Marek, Ondřej Ryšavý** a **Miroslav Švéda:** Multicast, TRILL and LISP Extensions for INET. Fakulta informačních technologií Vysoké učení technické v Brně (FIT VUT), 2014. Dostupné z: https://www.fit.vut.cz/research/publication-file/10901/clanek-cr5.pdf

[18] **Donald Eastlake, Mingui Zhang, Puneet Agarwal, Radia Perlman** a **Dinesh G. Dutt:** RFC 7172: Transparent Interconnection of Lots of Links (TRILL): Fine-Grained Labeling. Internet Engineering Task Force (IETF), květen 2014. Dostupné z: https://datatracker.ietf.org/doc/html/rfc7172

[19] **Edward Tetz:** Spanning Tree Protocol (STP) Introduction. Dummies. Dostupné z: https://www.dummies.com/programming/networking/cisco/spanning-tree-protocol-stp-introduction/

[20] **Ing. Miroslav Matuška, Ph.D:** TRILL 3. část – Pokročilé principy fungování. Lupa.cz, říjen 2010. Dostupné z: https://www.lupa.cz/clanky/trill-3-cast-pokrocile-principy-fungovani/

[21] **Autor neznámý:** Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches. Cisco, prosinec 2019. Dostupné z: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html

[22] **Autor neznámý:** Spanning-Tree Protocols User Guide. Juniper Networks, červen 2021. Dostupné z: https://www.juniper.net/documentation/us/en/software/junos/stp-l2/stp-l2.pdf

[23] **Autor neznámý:** Spanning Tree Protocols. Cisco, Dostupné z: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/spanning_tree.pdf

[24] **Petr Bouška:** Cisco IOS 9 - Spanning Tree Protocol. Samuraj-cz, květen 2009. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-9-spanning-tree-protocol/

[25] **Petr Bouška:** Cisco IOS 10 - Rapid Spanning Tree Protocol. Samuraj-cz, září 2007. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-10-rapid-spanning-tree-protocol/

[26] **Autor neznámý:** Compare and Contrast SPB and TRILL. Avaya, 2010. Dostupné z: http://www.techdata.ca/business/avaya/DataCenterSolutions/files/A%20-%20Why%20Avaya/2%20-%20Learn%20More%20About%20VENA/SPB-TRILL_Compare_Contrast-DN4634.pdf

[27] **Autor neznámý:** Shortest Path Bridging Architecture guide. Alcatel Lucent Enterprise, duben 2021. Dostupné z: https://www.al-enterprise.com/-/media/assets/internet/documents/spb-architecture-tech-brief-en.pdf

[28] **Mikael Holmberg:** TRILL vs. SPB. Extreme networks, Dostupné z: https://www.trex.fi/2014/xtrm-trill-vs-spb.pdf

[29] **Steve Brachmann:** The Evolution of the Internet: The spanning tree protocol, a major achievement in Internet routing. IPWatchdog, únor 2016. Dostupné z: https://www.ipwatchdog.com/2016/02/04/spanning-tree-protocol-internet-routing/id=65051/

[30] **Bc. Marcel Marek:** Modelování protokolů IS-IS a TRILL. Fakulta informačních technologií Vysoké učení technické v Brně (FIT VUT), květen 2013. Dostupné z: https://dspace.vutbr.cz/xmlui/bitstream/handle/11012/53511/final-thesis.pdf?sequence=6&isAllowed=y

[31] **Jiří Březina:** Evoluce protokolů pro zamezení vzniku smyček na linkové vrstvě. Fakulta elektrotechniky a komunikačních technologií Vysoké učení technické v Brně (FEKT VUT), červen 2020. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=210386

[32] **Stanislav Vodehnal:** Návrh datových sítí poskytovatelů připojení k Internetu. Fakulta elektrotechniky a komunikačních technologií Vysoké učení technické v Brně (FEKT VUT), červen 2016. Dostupné z: https://dspace.vutbr.cz/bitstream/handle/11012/61535/final-thesis.pdf?sequence=6&isAllowed=y

[33] **Vladimír Mandák:** Vizualizace Spanning Tree Protocol. Západočeská univerzita v Plzni Fakulta aplikovaných věd Katedra informatiky a výpočetní techniky, červen 2015. Dostupné z: https://otik.uk.zcu.cz/bitstream/11025/17873/1/DPA12N0030P.pdf

[34] **Milan Novotný:** Úlohy pro předmět Distribuované systémy a lokální počítačové sítě II. Vysoká škola podnikání a práva Katedra aplikované informatiky, listopad 2017

[35] **Nasir Khan** a **Zard Ali Khan:** Comparative Analysis of Trill: A Research Study. Department of Information Technology University of Haripur, září 2017. Dostupné z: https://www.researchgate.net/publication/330888235_Comparative_Analysis_of_Trill_A_Research_Study

[36] **Autor neznámý:** Spanning Tree Protocols: STP, RSTP, and MSTP – Feature overview and configuration guide. Allied Telesis, 2015. Dostupné z:

https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/stp_feature_config_guide.pdf

[37] **Autor neznámý:** Management Software AT-S63 Features Guide For Stand-alone AT-9400 Switches and AT-9400Ts Stacks. Allied Telesis, 2009. Dostupné z: https://www.alliedtelesis.com/sites/default/files/documents/installation-guides/s63_v410_features_guide.pdf

[38] **Gary A. Donahue:** Kompletní průvodce síťového experta. Computer Press, 2009. ISBN 978-80-251-2247-1.

[39] **Autor neznámý:** Počítačové sítě. Internet a jeho služby. Dostupné z: http://ijs2.8u.cz/index.php?option=com_content&view=category&layout=blog&id=8&Itemid=102

[40] **Libor Dostálek** a **Alena Kabelová:** Velký průvodce protokoly TCP/IP

a systémem DNS. Computer Press, 2000. ISBN 80-7226-323-4

[41] **Autor neznámý:** What Is a Data Center. Cisco, Dostupné z: https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html

[42] **Autor neznámý:** Rapid Spanning Tree Protocol (RSTP). Accuenergy, Dostupné z: https://www.accuenergy.com/support/reference-directory/rapid-spanning-tree-protocol-rstp/

[43] **Petr Bouška:** Počítačové sítě a jejich typy. Samuraj-cz, červenec 2007. Dostupné z: https://www.samuraj-cz.com/clanek/pocitacove-site-a-jejich-typy/

[44] **Petr Bouška:** VLAN – Virtual Local Area Network. Samuraj-cz, červen 2007. Dostupné z: https://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

[45] **Petr Bouška:** Cisco Routing 1 - obecné vlastnosti směrovacích protokolů. Samuraj-cz, březen 2009. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-routing-1-obecne-vlastnosti-smerovacich-protokolu/

[46] **Petr Bouška:** Cisco Routing 4 - IS-IS - Intermediate System to Intermediate System. Samuraj-cz, duben 2009. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-routing-4-is-is-intermediate-system-to-intermediate-system/

[47] **Petr Bouška:** Cisco Routing 3 - OSPF - Open Shortest Path First. Samuraj-cz, duben 2009. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-routing-3-ospf-open-shortest-path-first/

[48] **Autor neznámý:** Per-VLAN Spanning Tree (PVST) and Per-VLAN Spanning Tree Plus (PVST+). OmniSecu, Dostupné z: https://www.omnisecu.com/cisco-certified-network-associate-ccna/per-vlan-spanning-tree-pvst-and-per-vlan-spanning-tree-plus-pvst+.php

[49] **Yaw Hon Sing:** HOW TO INSTALL HUAWEI ENSP NETWORK SIMULATOR. Infosyte, Dostupné z: https://infosyte.com/how-to-install-huawei-ensp-

network-simulator/?fbclid=IwAR3Te_U7tR8n2yCO_ta3C7wMXw_mZ8tbB5IJOTs3fQip-1p5SKt_FmC4iv4

[50] **Autor neznámý:** CX320 Switch Module V100R001 Configuration Guide 10. Huawei, únor 2021. Dostupné z: https://support.huawei.com/enterprise/en/doc/EDOC1000128406/e33db6a1/configuration-examples

[51] **Autor neznámý:** 15-TRILL Configuration Guide. H3C Technologies, Dostupné z: http://www.h3c.com/en/Support/Resource_Center/HK/Switches/H3C_S10500/H3C_S10500/Technical_Documents/Configure/Configuration_Guide/H3C_S10500_CG-R7523P01-6W100/15/201609/951148_294551_0.htm

[52] **Lukáš Tesař:** Switche a VLANy. Dostupné z: https://tlukas.eu/uvod/switche-a-vlany

[53] **Matt Conran:** WHAT IS FABRICPATH, Network-Insight, srpen 2014. Dostupné z: https://network-insight.net/2014/08/what-is-fabricpath/

[54] **Autor neznámý:** Network Topology Architectures. IPCisco, Dostupné z: https://ipcisco.com/lesson/network-topology-architectures/

[55] **Autor neznámý:** OSPF. Katedra informatiky VŠB-TU, Dostupné z: http://www.cs.vsb.cz/grygarek/SPS/lect/OSPF/ospf.html#10

[56] **Autor neznámý:** IS-IS Overview. Juniper Networks, červen 2021, Dostupné z: https://www.juniper.net/documentation/us/en/software/junos/is-is/topics/concept/is-is-routing-overview.html

[57] **Eric Michel, Mbieda Petmegni Duplex Steve** a **Michael Ekonde Sone:** WLAN simulations using Huawei eNSP for e-laboratory in engineering schools. ResearchGate, duben 2020, Dostupné z: https://www.researchgate.net/publication/340949947_WLAN_simulations_using_Huawei_eNSP_for_e-laboratory_in_engineering_schools

[58] **Jiří Petrka:** Referenční model ISO/OSI - sedm vrstev. eArchiv.cz, Dostupné z: https://www.earchiv.cz/a92/a213c110.php3

Příloha A – Konfigurace RBridge1

```
#
sysname RBridge1
#
device board 1 board-type CE-MPUB
#
vlan batch 50 100
#
trill
 maximum load-balance 1
 network-entity 00.0000.0000.1111.00
 nickname 100
 carrier-vlan 10
 admin-vlan 50
 ce-vlan 100
#
aaa
 #
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
 #
 domain default_admin
#
interface Vlanif50
```

```
 ip address 192.168.10.1 255.255.255.0
#
interface MEth0/0/0
 undo shutdown
#
interface GE1/0/0
 undo shutdown
 port default vlan 100
#
interface GE1/0/1
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/2
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/3
 shutdown
#
interface GE1/0/4
 shutdown
#
interface NULL0
#
```

```
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr aes256_
cbc aes128_cbc 3des_cbc
#
ssh server dh-exchange min-len 1024
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr aes256_
cbc aes128_cbc 3des_cbc
#
user-interface con 0
#
vm-manager
#
return
```

Příloha B – Konfigurace RBridge2

```
#
sysname RBridge2
#
device board 1 board-type CE-MPUB
#
vlan batch 50 100
#
trill
 network-entity 00.0000.0000.2222.00
 nickname 200
 carrier-vlan 10
 admin-vlan 50
 ce-vlan 100
#
aaa
 #
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
 #
 domain default_admin
#
interface Vlanif50
 ip address 192.168.10.2 255.255.255.0
#
interface MEth0/0/0
```

```
 undo shutdown
#
interface GE1/0/0
 undo shutdown
 port default vlan 100
#
interface GE1/0/1
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/2
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/3
 shutdown
#
interface NULL0
#
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr aes256_
cbc aes128_cbc 3des_cbc
#
ssh server dh-exchange min-len 1024
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr aes256_
```

cbc aes128_cbc 3des_cbc

#

user-interface con 0

#

vm-manager

#

Return

Příloha C – Konfigurace RBridge3

```
#
sysname RBridge3
#
device board 1 board-type CE-MPUB
#
vlan batch 50 100
#
trill
 network-entity 00.0000.0000.3333.00
 nickname 300
 carrier-vlan 10
 admin-vlan 50
 ce-vlan 100
#
aaa
 #
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
 #
 domain default_admin
#
interface Vlanif50
 ip address 192.168.10.3 255.255.255.0
#
interface MEth0/0/0
```

```
 undo shutdown
#
interface GE1/0/0
 undo shutdown
 port default vlan 100
#
interface GE1/0/1
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/2
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/3
 shutdown
#
interface NULL0
#
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr aes256_
cbc aes128_cbc 3des_cbc
#
ssh server dh-exchange min-len 1024
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr aes256_
```

cbc aes128_cbc 3des_cbc

#

user-interface con 0

#

vm-manager

#

Return

Příloha D – Konfigurace RBridge4

```
#
sysname RBridge4
#
device board 1 board-type CE-MPUB
#
vlan batch 50 100
#
trill
 network-entity 00.0000.0000.4444.00
 nickname 400
 carrier-vlan 10
 admin-vlan 50
 ce-vlan 100
#
aaa
 #
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
 #
 domain default_admin
#
interface Vlanif50
 ip address 192.168.10.4 255.255.255.0
#
interface MEth0/0/0
```

```
 undo shutdown
#
interface GE1/0/0
 undo shutdown
 port default vlan 100
#
interface GE1/0/1
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/2
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/3
 shutdown
#
interface NULL0
#
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr aes256_
cbc aes128_cbc 3des_cbc
#
ssh server dh-exchange min-len 1024
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr aes256_
```

cbc aes128_cbc 3des_cbc

#

user-interface con 0

#

vm-manager

#

Return

Příloha E – Konfigurace RBridge5

```
sysname RBridge5
#
device board 1 board-type CE-MPUB
#
vlan batch 50
#
trill
 network-entity 00.0000.0000.5555.00
 nickname 500 root-priority 65535
 carrier-vlan 10
 admin-vlan 50
#
aaa
 #
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
 #
 domain default_admin
#
interface Vlanif50
 ip address 192.168.10.5 255.255.255.0
#
interface MEth0/0/0
 undo shutdown
#
```

```
interface GE1/0/0
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/1
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/2
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/3
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/4
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/5
```

```
 shutdown
#
interface NULL0
#
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr aes256_
cbc aes128_cbc 3des_cbc
#
ssh server dh-exchange min-len 1024
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr aes256_
cbc aes128_cbc 3des_cbc
#
user-interface con 0
#
vm-manager
#
Return
```

Příloha F – Konfigurace RBridge6

```
sysname RBridge6
#
device board 1 board-type CE-MPUB
#
vlan batch 50
#
trill
 network-entity 00.0000.0000.6666.00
 nickname 600 root-priority 65535
 carrier-vlan 10
 admin-vlan 50
#
aaa
 #
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
 #
 domain default_admin
#
interface Vlanif50
 ip address 192.168.10.6 255.255.255.0
#
interface MEth0/0/0
 undo shutdown
#
```

```
interface GE1/0/0
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/1
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/2
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/3
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/4
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/5
```

```
 shutdown
#
interface NULL0
#
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr aes256_
cbc aes128_cbc 3des_cbc
#
ssh server dh-exchange min-len 1024
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr aes256_
cbc aes128_cbc 3des_cbc
#
user-interface con 0
#
vm-manager
#
Return
```

Příloha G – Konfigurace RBridge7

```
sysname RBridge7
#
device board 1 board-type CE-MPUB
#
vlan batch 50
#
trill
 network-entity 00.0000.0000.7777.00
 nickname 700 root-priority 65535
 carrier-vlan 10
 admin-vlan 50
#
aaa
 #
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
 #
 domain default_admin
#
interface Vlanif50
 ip address 192.168.10.7 255.255.255.0
#
interface MEth0/0/0
 undo shutdown
#
```

```
interface GE1/0/0
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/1
 undo shutdown
 port link-type trunk
 undo port trunk allow-pass vlan 1
 trill enable
#
interface GE1/0/2
 shutdown
#
interface NULL0
#
ssh authorization-type default aaa
#
ssh server cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr aes256_
cbc aes128_cbc 3des_cbc
#
ssh server dh-exchange min-len 1024
#
ssh client cipher aes256_gcm aes128_gcm aes256_ctr aes192_ctr aes128_ctr aes256_
cbc aes128_cbc 3des_cbc
#
user-interface con 0
#
vm-manager
#
```

return

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání diplomové práce

Autor: **Bc. Jonáš Horáček**

Studium: I1900299

Studijní program: N0688A140001 Informační management

Studijní obor:

Název diplomové práce: **Protokol TRILL a jeho využití v sítích LAN**

Název diplomové práce AJ: TRILL protocol and its use in LANs

Cíl, metody, literatura, předpoklady:

Cílem práce je podrobně popsat principy protokolu TRILL a analyzovat možnosti jeho nasazení v podnikové síti. Autor podrobně představí principy fungování protokolu TRILL. Autor připraví simulaci fungování protokolu TRILL a jeho využití v podnikové síti. V praktické části autor vytvoří case study pro nasazení protokolu TRILL s důrazem na vysokou dostupnost požadovaných služeb.

HOODA, Sanjay K., Shyam KAPADIA a Padmanabhan KRISHNAN. *Using TRILL, FabricPath and VXLAN: [designing massively scalable data centers with overlays]*. Indianapolis, IN: Cisco Press, [2014]. ISBN 9781587143939.

LIU, Yang. *Data center networks*. New York: Springer, 2013. ISBN 9783319019482.

Garantující pracoviště: Katedra informačních technologií,
Fakulta informatiky a managementu

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Oponent: Ing. Tomáš Svoboda, Ph.D.

Datum zadání závěrečné práce: 21.10.2019